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.: F19579

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 mayo 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
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 mayo 2021.

FECHA DE RECEPCIÓN: mayo 2021

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

No. DE FACTURA: F19579

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 19579

Folio Fiscal	C65CC442-F7B7-482E-9501-66AA64AF17C6
Fecha Emisión	2021-06-14T00:00:00
Fecha Certificación	2021-06-14T18:34:24
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

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

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

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 mayo 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

hGP60PeMg90OYenbfxOLY7T3lBJRxvNwDr6lO0ZMkdjjFsTBIsdPrj/xwLGxe2oyu87H5AiRcER92tKE0s1d1pL3PIR0A25an3ldE1/apdazyigg758prh0jp9lb+z82+JOY2wS0mvE+hdn08LaN9+HFAWf7SF1SQ/0CavIJGMopaEVtq+qb65bZGOZqBkQ+Jl7UpGVZqBQuokCR4/Zlj4jxeIA6jRy+5zx3cgwSln+hVhjbamcojRGB67Ab68Q6t7+ikj2StufMIbfJmRSxrJlFPAyZ+6x01EjMsMbzWJ+TIdNtkgN43Dj+N9pb5ilSGl3/Y/kGGzVyWh2fvRydnA==

Sello digital del SAT

SS7NDDmbHrfezvvTD1BGfSg7DgaNYabAtP2fgjRuD/AgIJ2l1Y7q4mg47rTKJ/dJjBrNmmiYrkitrWm6BNKZoz8Z2IquNW8aHBk7tKgLZc8MPKHDmu+HOcCKSk1VT68e05S3fVUXY2nwuEiYvboCkcmh5fQ4Y1GAwnZOA0N5HUW33LXT3yDo5Diyu1ug9yJjk4/AmKPYFV12B2sDGSRYJmO5XL9K3ilRDf5+VNmFka6ElmuTfhGL3sCV9mav3nNoPN61kdFNxlRVacjY6GumAOzZQkk3+UJZ+szLY9Rx1Msn8uFlAGWnHf0wla7yo1pEfADsig0w3ZPFFSw+MUXrGA==

Cadena original del complemento de certificación digital del SAT

||1.1|C65CC442-F7B7-482E-9501-66AA64AF17C6|2021-06-14T18:34:24|TLE011122SC2|hGP60PeMg90OYenbfxOLY7T3lBJRxvNwDr6lO0ZMkdjjFsTBIsdPrj/xwLGxe2oyu87H5AiRcER92tKE0s1d1pL3PIR0A25an3ldE1/apdazyigg758prh0jp9lb+z82+JOY2wS0mvE+hdn08LaN9+HFAWf7SF1SQ/0CavIJGMopaEVtq+qb65bZGOZqBkQ+Jl7UpGVZqBQuokCR4/Zlj4jxeIA6jRy+5zx3cgwSln+hVhjbamcojRGB67Ab68Q6t7+ikj2StufMIbfJmRSxrJlFPAyZ+6x01EjMsMbzWJ+TIdNtkgN43Dj+N9pb5ilSGl3/Y/kGGzVyWh2fvRydnA==|00001000000503270882||

Recepción de compra

Número recepción de compra: RECEP-21-1083
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-21-1127
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-21-1083

Número factura compra: F19579
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-21-1127
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	3,566.97	3,566.97
	013	31603	1	12	MATERIALES INDIRECTOS	SER	1	4,161.47	4,161.47
	013	31603	1	13	MATERIALES INDIRECTOS	SER	1	7,728.44	7,728.44
	013	31603	1	21	MATERIALES INDIRECTOS	SER	1	1,188.99	1,188.99
	013	31603	1	22	MATERIALES INDIRECTOS	SER	1	16,645.86	16,645.86
	013	31603	1	23	MATERIALES INDIRECTOS	SER	1	10,106.42	10,106.42
	013	31603	1	24	MATERIALES INDIRECTOS	SER	1	5,944.95	5,944.95
	013	31603	1	31	GASTOS DE VENTA	SER	1	1,188.99	1,188.99
	013	31603	1	32	GASTOS DE VENTA	SER	1	5,350.46	5,350.46
	001	31603	1	41	GASTOS DE ADMINISTRACION	SER	1	1,783.49	1,783.49
	001	31603	1	42	GASTOS DE ADMINISTRACION	SER	1	40,425.67	40,425.67
	001	31603	1	43	GASTOS DE ADMINISTRACION	SER	1	16,051.37	16,051.37
	013	31603	1	51	MATERIALES INDIRECTOS	SER	1	7,133.94	7,133.94
	013	31603	1	52	MATERIALES INDIRECTOS	SER	1	16,051.37	16,051.37
	013	31603	1	53	MATERIALES INDIRECTOS	SER	1	20,212.83	20,212.83
	013	31603	1	54	GASTOS DE ADMINISTRACION	SER	1	2,972.43	2,972.43
	001	31603	1	61	GASTOS DE ADMINISTRACION	SER	1	5,944.93	5,944.93

Subtotal: **166,458.58**
Descuento factura: 0.00
IVA: 26,633.37

Total de MXN: **193,091.95**

Autorización de pago

RAUL YAU

SUBDIRECTOR GENERAL TECNICO
Y OPERATIVO

Presente:

No.: SP-21-01493

No. Autorización: SP-21-01493

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.)

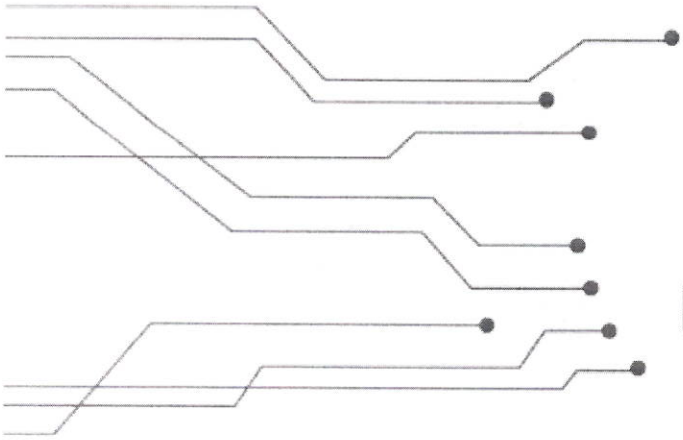
Por el pago que se indica en la Solicitud de Pago número SP-21-01493

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 mayo 2021.



INFOTEC

Reporte de Incidentes y Solicitudes de Mesa de Servicio

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

MAYO 2021

Información general del documento

Entregable

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

Elaboración

Puesto	Nombre	Firma	Fecha
Supervisor de Mesa de Servicio	Gerardo Diego Huerta Clemente		01/06/2021

Revisión

Puesto	Nombre	Firma	Fecha
Coordinador de Mesa de Servicio	Alejandro Rubén de la Cruz		01/06/2021

Aprobación

Puesto	Nombre	Firma	Fecha
Líder de Proyecto	Victor Quiroz Barrientos		01/06/2021

Recepción Cliente

Puesto	Nombre	Firma	Fecha
Gerente de Tecnologías de la Información	Ing. Juan Pablo Rosas Turanzas		16-~~06~~-Jun-2021

Aprobación Cliente

Puesto	Nombre	Firma	Fecha
Jefe de Unidad Departamental	Ing. Emilio René García Rodríguez		16-Jun-2021

Introducción al documento.

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

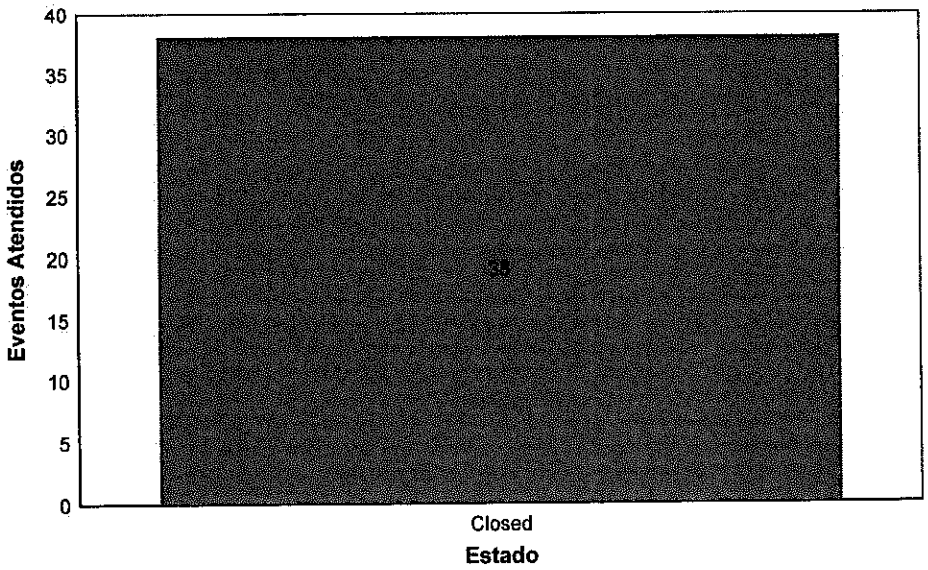
Atentamente.

Mesa Central de Servicios INFOTEC
Dirección Adjunta de Desarrollo Tecnológico.

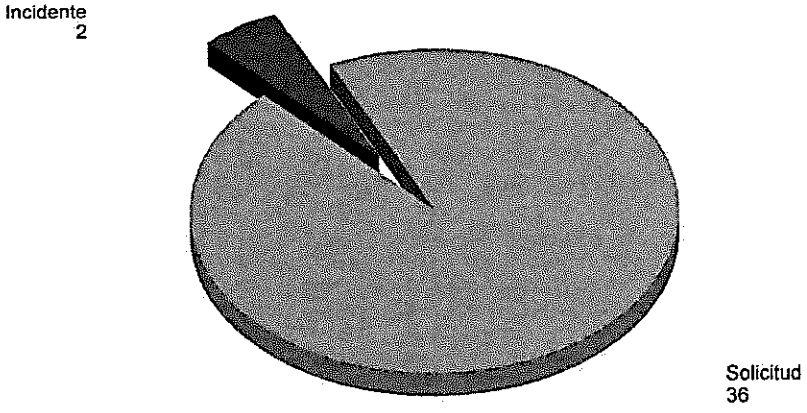
CANAL 22

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

Estado de Eventos



Tipo de Eventos



Nota:
Solicitud de Servicio se deberá entender como Requerimiento.

CANAL 22

Detalle de Eventos

Título: ALERTA CANAL 22 / http://programa.canal22.org.mx/ URL NO RESPONDE

Descripción:
CLIENTE: CANAL 22
URL: http://programa.canal22.org.mx/
ALERTA: URL NO RESPONDE

Atendido por: CARLOS CRUZ, ELIDETH
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 10/05/2021 10:17:14p.m.
Ticket asignado: TK313417
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 10/0572021 22;25 Hrs. En atencion al evento se valida con el Ing. Emilio Garcia de CANAL 22 y que la URL responde correctamente y se da por atendido el TK.

Fecha y hora de cierre: 10/05/2021 10:46:49p.m.
Tiempo total del Ticket: 00 00:29:35

Título: ALERTA CANAL22/ noticias.canal22.org.mx / URL NO RESPONDE
Descripción: Por medio de la presente se reporta la siguiente alerta de monitoreo

CLIENTE: CANAL22
URL: noticias.canal22.org.mx
ALERTA: URL NO RESPONDE

Atendido por: VAZQUEZ FLORES, LUIS NOE
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 27/05/2021 04:01:45a.m.
Ticket asignado: TK314171
Medio de contacto: Correo electronico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 27/05/2021 04:07 Hrs. En atención al evento se reciben comentarios por parte del Ing. Isis Rodriguez de Monitoreo:

URL RESPONDE CORRECTAMENTE

ANEXO EVIDENCIA

Fecha y hora de cierre: 27/05/2021 04:09:23a.m.
Tiempo total del Ticket: 00 00:07:38

Título: Reporte de consumo de ancho de banda-2021-05-01-1000_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: GUEVARA MORALES, TERESA_.
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 01/05/2021 11:02:31a.m.
Ticket asignado: TK313039
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 01/05/2021 11:05 Hrs. En atención al evento se reciben comentarios por parte del Área del SOC:
Se adjunta el reporte.

Fecha y hora de cierre: 03/05/2021 04:34:21p.m.
Tiempo total del Ticket: 02 05:31:50

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

Se adjunta el reporte.

CANAL 22

Detalle de Eventos

Atendido por:	RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	02/05/2021 10:07:55a.m.
Ticket asignado:	TK313050
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

Solución: 02/05/2021 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 TK313050, solicitando de su apreciable apoyo para brindar atención al evento que se describe en el correo que antecede.

Fecha y hora de cierre:	03/05/2021 04:33:24p.m.
Tiempo total del Ticket:	01 06:25:29

Título:	Reporte de consumo de ancho de banda-2021-05-03-1000_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:	03/05/2021 10:03:20a.m.
Ticket asignado:	TK313065
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

Solución: 03/05/2021 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:	03/05/2021 04:32:20p.m.
Tiempo total del Ticket:	00 06:29:00

CANAL 22

Detalle de Eventos

Título:	Cambio DNS CANAL 22
Descripción:	Estimados

Buen día,

Solicito su ayuda para realizar el cambio en un nombre de dominio, adjunto el formato para altas cambios y modificaciones de DNS

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:	03/05/2021 11:08:36a.m.
Ticket asignado:	TK313069
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	03/05/2021 12:18 Hrs. En atención al evento se reciben comentarios del Ing. Anabel Jeronimo de Adminweb : Les informo que se dio de alta el siguiente registro:

Y se actualizo el siguiente:

Fecha y hora de cierre:	04/05/2021 07:04:06p.m.
Tiempo total del Ticket:	01 07:55:30

CANAL 22

Detalle de Eventos

Título: Certificado SSL defensoria_Canal_22

Descripción: Solicito su ayuda para colocar los certificados SSL que envió adjuntos al portal de defensoria.canal22.org.mx con el siguiente direccionamiento

IP Publica

WAF

IP Interna

Puertos

189.204.131.141

10.0.0.216

172.20.22.43

TCP: 80 --> 443

Atendido por: GUEVARA MORALES, TERESA_.
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 03/05/2021 12:53:46p.m.
Ticket asignado: TK313081
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 03/05/2021 16:30 Hrs. En atención al evento le hacemos llegar los comentarios del Ing. Efrain Nochebuena SOC.

Se cargo el certificado en el equipo WAF

Fecha y hora de cierre: 03/05/2021 07:14:14p.m.
Tiempo total del Ticket: 00 06:20:28

CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-05-04-1000_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: RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 04/05/2021 10:06:08a.m.
Ticket asignado: TK313133
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 04/05/2021 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: 06/05/2021 02:30:49p.m.
Tiempo total del Ticket: 02 04:24:41

Título: Reporte de consumo de ancho de banda-2021-05-05-1000_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: 05/05/2021 10:04:59a.m.
Ticket asignado: TK313209
Medio de contacto: Correo electronico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

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

Se adjunta el reporte.

Fecha y hora de cierre: 05/05/2021 08:03:07p.m.
Tiempo total del Ticket: 00 09:58:08

Título: Reporte de consumo de ancho de banda-2021-05-06-1000
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: 06/05/2021 10:07:46a.m.
Ticket asignado: TK313244
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 06/05/2021 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 TK313244, solicitando de su apreciable apoyo para brindar atención al evento que se describe en el correo que antecede.

Fecha y hora de cierre: 06/05/2021 02:29:47p.m.
Tiempo total del Ticket: 00 04:22:01

CANAL 22

Detalle de Eventos

Título:	Reporte de consumo de ancho de banda-2021-05-07-1000 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:	07/05/2021 10:05:10a.m.
Ticket asignado:	TK313301
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	07/05/2021 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:	07/05/2021 11:49:44a.m.
Tiempo total del Ticket:	00 01:44:34

CANAL 22

Detalle de Eventos

Título: Certificado SSL noticias.canal22.org.mx_CANAL_22

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

Nombre Publicado Firewall

IP Publica

WAF

IP Interna

Puertos

Noticias

189.204.131.139

10.0.0.211

172.20.22.19

(TCP: 443 –> 443)
(TCP: 80 –> 80)

Adjunto el certificado y quedo al pendiente de cuaqluier duda o aclaración.

Atendido por: RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 07/05/2021 01:14:47p.m.
Ticket asignado: TK313318
Medio de contacto: Correo electronico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 12/05/2021 12:25 Hrs. En atención al evento se reciben comentarios del Ing. Efrain Nochebuena de SOC

Se actualizo el certificado ssl

Fecha y hora de cierre: 12/05/2021 03:41:17p.m.
Tiempo total del Ticket: 05 02:26:30

Título: Reporte de consumo de ancho de banda-2021-05-08-1000_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: RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 08/05/2021 10:05:22a.m.
Ticket asignado: TK313362
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 08/05/2021 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 TK313362, solicitando de su apreciable apoyo para brindar atención al evento que se describe en el correo que antecede.

Fecha y hora de cierre: 09/05/2021 09:59:51p.m.
Tiempo total del Ticket: 01 11:54:29

Título: Reporte de consumo de ancho de banda-2021-05-09-1000_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.

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:	09/05/2021 10:02:09a.m.
Ticket asignado:	TK313370
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

Solución:
SOC:

09/05/2021 10:05 Hrs. En atención al evento se reciben comentarios por parte del Área del

Se adjunta el reporte.

Fecha y hora de cierre:	09/05/2021 10:01:09p.m.
Tiempo total del Ticket:	00 11:59:00

Título:	Reporte de consumo de ancho de banda-2021-05-10-1000
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:	10/05/2021 10:07:28a.m.
Ticket asignado:	TK313383
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

CANAL 22

Detalle de Eventos

Solución: 10/05/2021 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: 10/05/2021 01:08:24p.m.
Tiempo total del Ticket: 00 03:00:56

Título: Reporte de consumo de ancho de banda-2021-05-11-1000_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.

Atendido por: GONZALEZ CURENO, ROGELIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 11/05/2021 10:05:20a.m.
Ticket asignado: TK313424
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 11/05/2021 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: 12/05/2021 12:32:04p.m.
Tiempo total del Ticket: 01 02:26:44

Título: Reporte de consumo de ancho de banda-2021-05-12-1000_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:	GONZALEZ CURENO, ROGELIO
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	12/05/2021 10:07:32a.m.
Ticket asignado:	TK313484
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

Solución: 11/05/2021 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:	12/05/2021 12:32:25p.m.
Tiempo total del Ticket:	00 02:24:53

Título:	Reporte de consumo de ancho de banda-2021-05-13-1000_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.
Atendido por:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	13/05/2021 10:10:09a.m.
Ticket asignado:	TK313551
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

Solución: 13/05/2021 10:17 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre:	13/05/2021 01:20:50p.m.
Tiempo total del Ticket:	00 03:10:41

CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-05-14-1000 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: 14/05/2021 10:26:34a.m.
Ticket asignado: TK313604
Medio de contacto: Correo electronico
Estado evento: Cerrado
Solución: 14/05/2021 10:17 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 14/05/2021 05:52:50p.m.
Tiempo total del Ticket: 00 07:26:16

Título: Reporte de consumo de ancho de banda-2021-05-15-1000
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: 15/05/2021 10:06:46a.m.
Ticket asignado: TK313657
Medio de contacto: Correo electronico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 15/05/2021 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 TK313657 solicitando de su apreciable apoyo para brindar atención al evento que se describe en el correo que antecede.

Fecha y hora de cierre: 17/05/2021 11:39:27a.m.
Tiempo total del Ticket: 02 01:32:41

Título: Reporte de consumo de ancho de banda-2021-05-16-1000_CANAL_22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: GUEVARA MORALES, TERESA_.
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 16/05/2021 10:02:30a.m.
Ticket asignado: TK313675
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 16/05/2021 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: 17/05/2021 09:05:39p.m.
Tiempo total del Ticket: 01 11:03:09

CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-05-18-1000 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: 18/05/2021 10:18:34a.m.
Ticket asignado: TK313755
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 18/05/2021 10:23 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 18/05/2021 03:52:26p.m.
Tiempo total del Ticket: 00 05:33:52

Título: Reporte de consumo de ancho de banda-2021-05-19-1000_Canal_22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: GUEVARA MORALES, TERESA_.
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 19/05/2021 10:08:06a.m.
Ticket asignado: TK313814
Medio de contacto: Correo electronico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 19/05/2021 10:11 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 19/05/2021 02:00:08p.m.
Tiempo total del Ticket: 00 03:52:02

Título: Reporte de consumo de ancho de banda-2021-05-21-1000_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: GONZALEZ CURENO, ROGELIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 21/05/2021 10:06:07a.m.
Ticket asignado: TK313914
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 21/05/2021 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: 24/05/2021 09:17:57a.m.
Tiempo total del Ticket: 02 23:11:50

Título: Reporte de consumo de ancho de banda-2021-05-22-1000_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.

CANAL 22

Detalle de Eventos

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 22/05/2021 10:03:09a.m.
Ticket asignado: TK313972
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 22/05/2021 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: 24/05/2021 07:49:49p.m.
Tiempo total del Ticket: 02 09:46:40

Título: Reporte de consumo de ancho de banda-2021-05-23-1000_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.

Atendido por: GUEVARA MORALES, TERESA_.
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 23/05/2021 10:02:31a.m.
Ticket asignado: TK313981
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 23/05/2021 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: 24/05/2021 10:27:59a.m.
Tiempo total del Ticket: 01 00:25:28

CANAL 22

Detalle de Eventos

Título:	Reporte de consumo de ancho de banda-2021-05-24-1000_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:	24/05/2021 10:02:51a.m.
Ticket asignado:	TK313999
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución: SOC:	24/05/2021 10:00 Hrs. En atención al evento se reciben comentarios por parte del área del

Se adjunta el reporte.

Fecha y hora de cierre:	24/05/2021 07:50:36p.m.
Tiempo total del Ticket:	00 09:47:45

CANAL 22

Detalle de Eventos

Título: Edición cliente VPN CANAL 22

Descripción: Estimados

Buenos días.

Solicito su ayuda para modificar el siguiente cliente VPN agregando el acceso a la IP "172.31.201.64":

Nombre

Usuario

Contraseña

Acceso IP's

Ing. Pedro O. Rodríguez

pedro.rodriguez

p3dr0Rodr1gu3z*

10.100.1.0/24

172.31.201.64

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:	24/05/2021 10:14:45a.m.
Ticket asignado:	TK314001
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

Solución: 24/05/2021 10:43 Hrs. En atención al evento se reciben comentarios por parte del Ing. Efrain Nochebuena del SOC:

Se agrego la IP como destino en la política que permite el acceso al usuario de VPN pedro.rodriguez

Favor de validar el acceso.

Fecha y hora de cierre:	24/05/2021 07:51:01p.m.
Tiempo total del Ticket:	00 09:36:16

CANAL 22

Detalle de Eventos

Título: Modificar cliente VPN_CANAL 22
Descripción: Buenos días

Solicito su ayuda para modificar el siguiente cliente VPN y dar acceso a la IP 172.20.22.12

Nombre

Usuario

Contraseña

Acceso IP's

Claudia Rivera

claudia

cL4ud14TvC22

172.20.22.10
172.20.22.46
172.20.22.44
172.20.22.35

172.20.22.12

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: 25/05/2021 09:35:13a.m.
Ticket asignado: TK314067
Medio de contacto: Correo electronico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 25/05/2021 17:04 Hrs. En atención al evento se reciben comentarios del Ing. Efrain Nochebuena de SOC:

Se agrego IP en los permisos de comunicación.

Fecha y hora de cierre: 25/05/2021 07:52:40p.m.
Tiempo total del Ticket: 00 10:17:27

Título: Reporte de consumo de ancho de banda-2021-05-25-1000 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: 25/05/2021 10:10:09a.m.
Ticket asignado: TK314069
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 25/05/2021 10:00 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Fecha y hora de cierre: 25/05/2021 05:28:34p.m.
Tiempo total del Ticket: 00 07:18:25

CANAL 22

Detalle de Eventos

Título:	Reporte de consumo de ancho de banda-2021-05-26-1000_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:	26/05/2021 10:06:00a.m.
Ticket asignado:	TK314131
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	26/05/2021 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:	27/05/2021 03:58:28p.m.
Tiempo total del Ticket:	01 05:52:28

CANAL 22

Detalle de Eventos

Título: Modificación de clientes VPN CANAL 22

Descripción: Solicito su ayuda para dar acceso a la IP 172.20.22.43 a los siguientes clientes VPN:

Nombre

Usuario

Contraseña

Acceso IP's

José Luis Montiel

jose

j0s3C22*

172.20.22.10
172.20.22.46
172.20.22.44
172.20.22.35

172.20.22.43

Claudia Rivera

claudia

cL4ud14TvC22

172.20.22.10
172.20.22.46
172.20.22.44
172.20.22.35

172.20.22.43

Quedo al pendiente de cualquier duda o aclaración.

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:	27/05/2021 09:34:57a.m.
Ticket asignado:	TK314178
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	27/05/2021 15:55 Hrs. En atención al evento le hacemos llegar los comentarios del SOC.

Se agregó IP a los permisos de comunicación

Fecha y hora de cierre:	27/05/2021 07:05:59p.m.
Tiempo total del Ticket:	00 09:31:02

Título:	Reporte de consumo de ancho de banda-2021-05-27-1000
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.

Atendido por:	RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	27/05/2021 10:10:35a.m.
Ticket asignado:	TK314179
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	27/05/2021 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 TK314179 solicitando de su apreciable apoyo para brindar atención al evento que

Fecha y hora de cierre:	27/05/2021 03:59:35p.m.
Tiempo total del Ticket:	00 05:49:00

CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-05-28-1000_CANAL 22

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

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 28/05/2021 10:06:17a.m.
Ticket asignado: TK314214
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 28/05/2021 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: 28/05/2021 07:36:28p.m.
Tiempo total del Ticket: 00 09:30:11

Título: Reporte de consumo de ancho de banda-2021-05-29-1000

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: 29/05/2021 10:05:29a.m.
Ticket asignado: TK314278
Medio de contacto: Correo electronico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 29/05/2021 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 TK314278 solicitando de su apreciable apoyo para brindar atención al evento que se describe en el correo que antecede.

Fecha y hora de cierre: 31/05/2021 06:50:56p.m.
Tiempo total del Ticket: 02 08:45:27

Título: Reporte de consumo de ancho de banda-2021-05-30-1000_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.

Se adjunta el reporte.

Atendido por: GUEVARA MORALES, TERESA_.
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 30/05/2021 10:02:36a.m.
Ticket asignado: TK314289
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 30/05/2021 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: 31/05/2021 06:51:19p.m.
Tiempo total del Ticket: 01 08:48:43

Título: Reporte de consumo de ancho de banda-2021-05-31-1000_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:	31/05/2021 10:06:30a.m.
Ticket asignado:	TK314297
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	31/05/2021 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:	31/05/2021 06:52:31p.m.
Tiempo total del Ticket:	00 08:46:01

CANAL 22

Detalle de Eventos

Título: Modificación cliente VPN_CANAL 22

Descripción: Solicito su ayuda para modificar el siguiente cliente VPN y otorgar acceso a la IP 10.100.10.43.

Nombre

Usuario

Contraseña

Acceso IP's

Luis Ángel Noguez Fonseca

luis.noguez

lu1s.n0g3zC22

172.31.200.161

10.100.10.43

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 31/05/2021 10:08:37a.m.
Ticket asignado: TK314298
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 31/05/2021 12:23Hrs. En atencion al evento se reciben comentarios del ing. Efrain Nochebuena de SOC:
El usuario de VPN ya tiene permitido el acceso a toda la red 10.100.10.0/24

Fecha y hora de cierre: 31/05/2021 06:53:56p.m.
Tiempo total del Ticket: 00 08:45:19

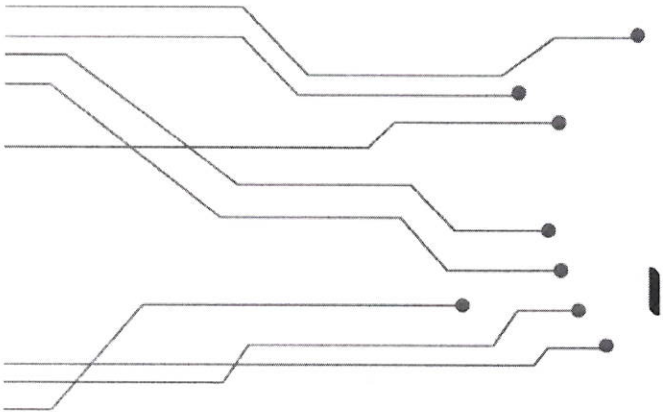
CANAL 22

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 acceso a Internet

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

MAYO 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		16-06-2021

Aprobación Cliente

Puesto	Nombre	Firma	Fecha
Jefe de Unidad Departamental	Ing. Emilio René García Rodríguez		16-06-2021

Tabla de contenido

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).

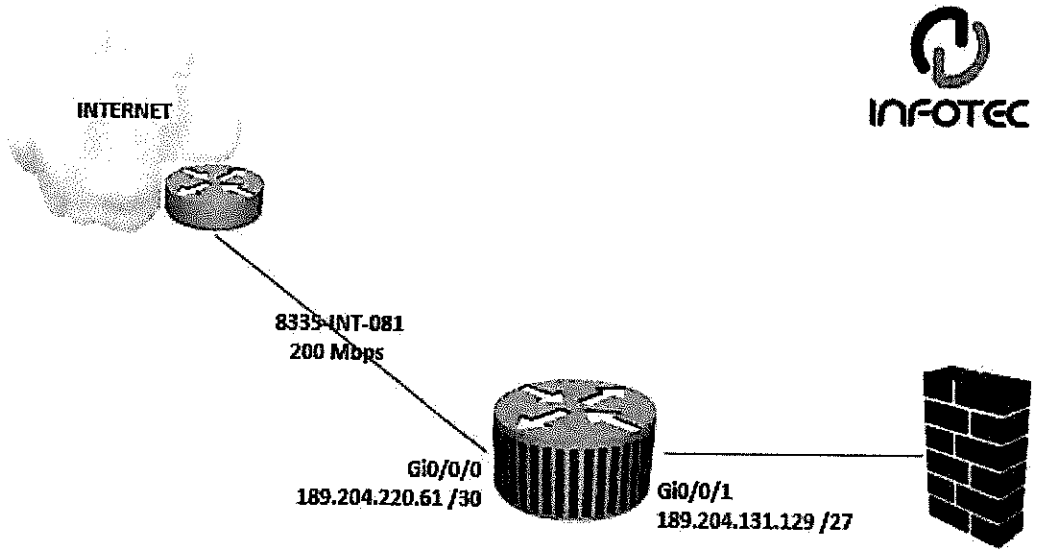
2. Objetivo

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 mayo de 2021 al 31 de mayo 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.

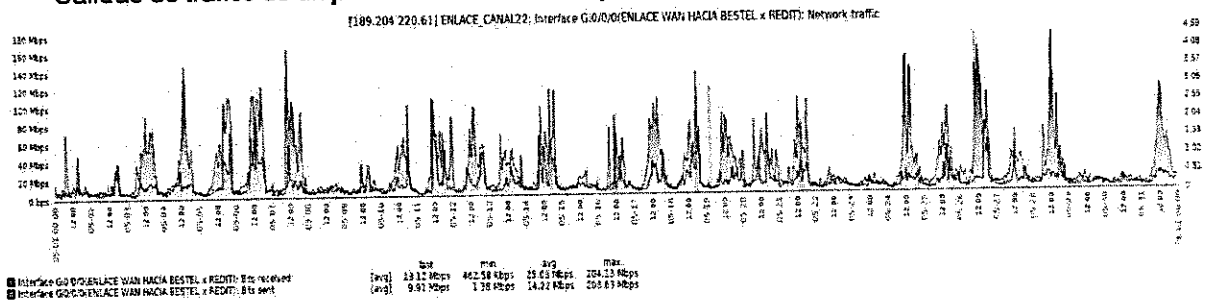
Red de Publicación a INTERNET		
VLAN	**DIRECCIONAMIENTO IP**	**DESCRIPCIÓN**
Por definir	189.204.131.128/27	Administración y Monitoreo

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.

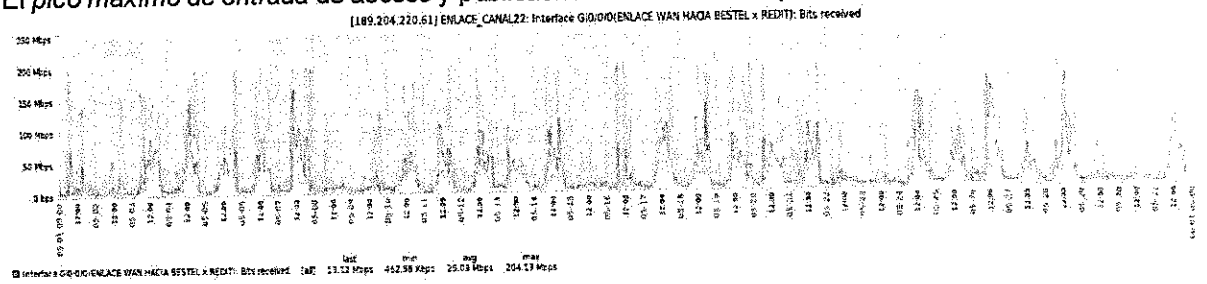
Durante el mes de mayo se presentaron los siguientes datos en la interface donde llega el enlace:

- Entradas de tráfico de un ***promedio*** de ***25.03 Mbps.***
- Salidas de tráfico de un ***promedio*** de ***14.22 Mbps.***



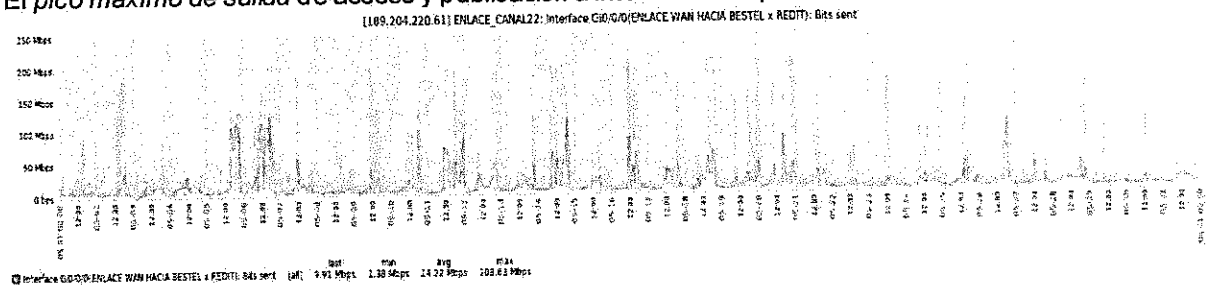
Trafico entrada

El *pico máximo de entrada* de acceso y publicación a internet correspondiente es de **204.13 Mbps.**

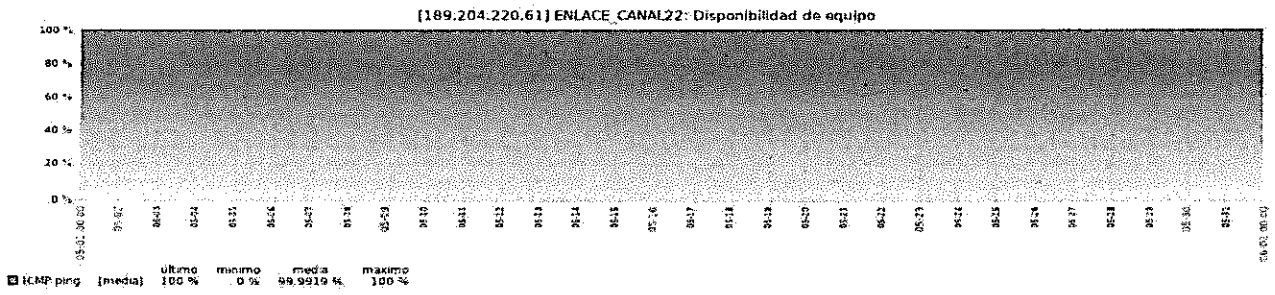


Trafico salida

El *pico máximo de salida* de acceso y publicación a internet correspondiente es de **208.63 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 especifica.

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.

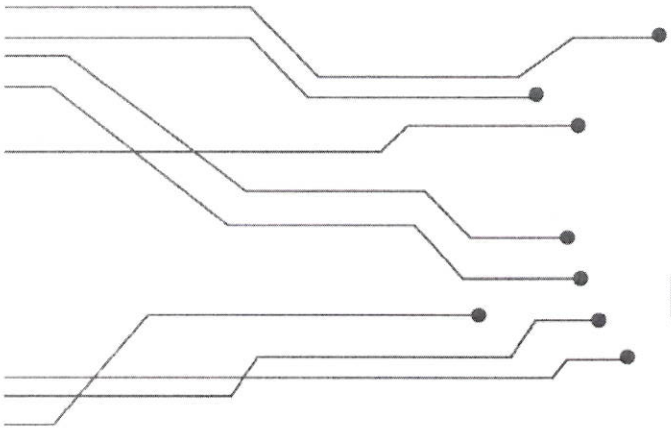
- Discard Exceptions (# de muestras)
- Discard Exceptions (% de muestras)

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)



INFOTEC

Reporte de Seguridad Perimetral UTM y Seguridad para Servidores Web

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

MAYO 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		16-jun-2021

Aprobación Cliente

Puesto	Nombre	Firma	Fecha
Jefe de Unidad Departamental	Ing. Emilio René García Rodríguez		16-06-2021

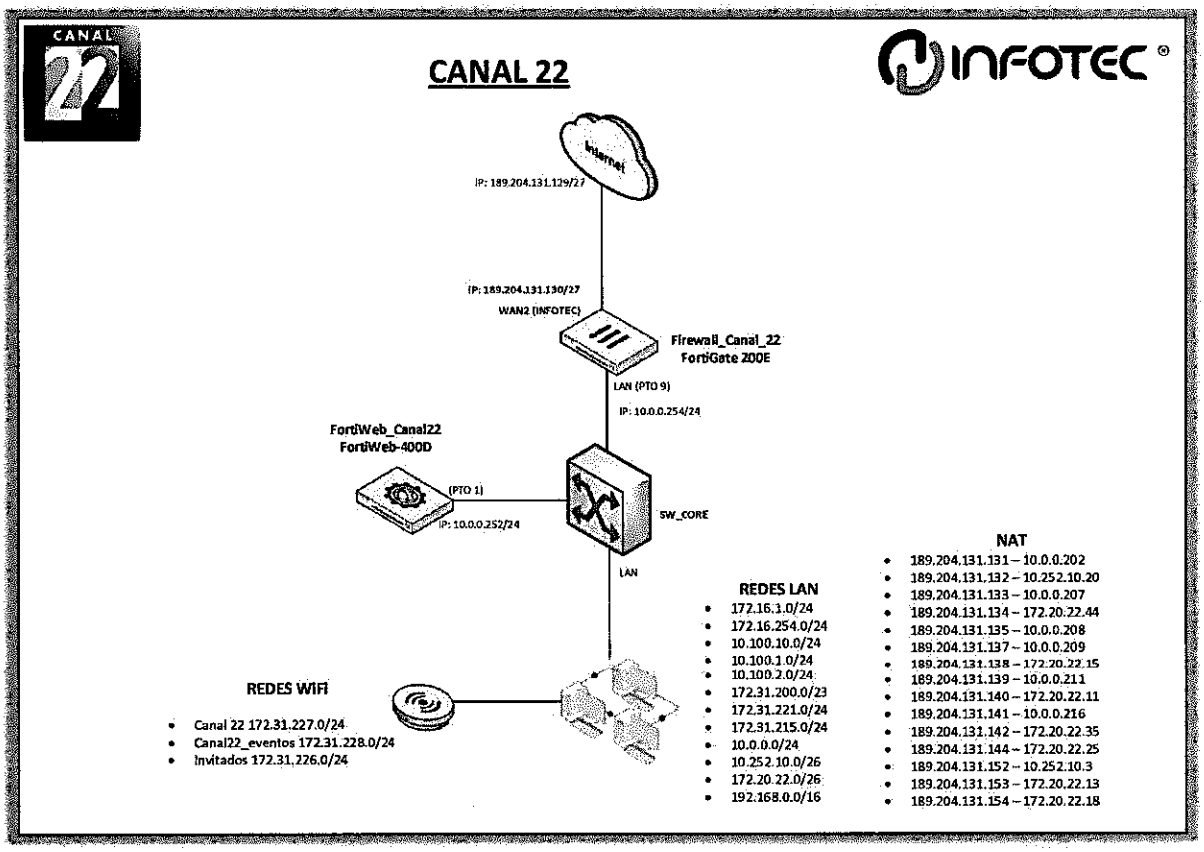
Tabla de contenido

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	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		189.240.110.183_Nba	ACCEPT
Red_Local (port9)	sd-wan	172.16.10.24 10.100.10.0/24	all	always	ALL		Enabled	ACCEPT
Red_Local (port9)	sd-wan	10.100.1.0/24 10.100.2.0/24	all	always	ALL		Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.31.220.241-172.31.220.248	all	always	ALL		Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.31.220.169/32 172.31.220.2-32 172.31.220.241-172.31.220.248 172.16.1.194-172.16.1.198 172.31.215.184-172.31.215.185	all	always	ALL		Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.31.210.33	all	always	ALL		Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.31.210.18/32 172.31.210.188/32	all	always	ALL		Enabled	ACCEPT
Canal 22 (canal22)	sd-wan	172.31.227.0/24	all	always	ALL		Enabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 SOC	10.0.0.252_WAF 10.0.0.25-32 10.0.0.0/24 172.20.22.0/24 10.0.0.1-10.0.0.251	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 sandra	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.abreo	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.alguin	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.noguez	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 erika	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 nevison	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	192.168.0.0/24 10.0.0.0/24 10.100.10.0/24 10.252.10.0/24 172.16.1.0/24 172.31.200.0/23 172.31.213.0/24 172.31.221.0/24	always	ALL		Enabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 leticiarreyes gzzonvalley promocar1 promocar2	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 10.100.1.0/24 172.31.201.64/32	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)	Ransomware	all	always	ALL			DENY
sd-wan	Red_Local (port9)	all	Mail_server_list_POP3 Mail_server_list_SMTP	always	POP3 SMTP		Disabled	ACCEPT
sd-wan	Red_Local (port9)	all	Desarrollo_443 Desarrollo Desarrollo_8080	always	8080-TCP HTTP HTTPS		Enabled	ACCEPT
sd-wan	Red_Local (port9)	all	Portal Proyectos Portal Proyectos_443	always	ALL_ICMP HTTP HTTPS		Disabled	ACCEPT
sd-wan	Red_Local (port9)	all	Noticias_php_443 Noticias_php_80	always	HTTP ALL_ICMP HTTPS		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		Enabled	ACCEPT
sd-wan	Red_Local (port9)	all	Publicacion_Canal22-80 Publicacion_Canal22-443	always	HTTP ALL_ICMP HTTPS TRACEROUTE		Enabled	ACCEPT
sd-wan	Red_Local (port9)	all	Subdominios canal22	always	HTTP HTTPS PING		Enabled	ACCEPT
sd-wan	Red_Local (port9)	all	Portal_Clic_Clac	always	HTTP ALL_ICMP HTTPS		Enabled	ACCEPT

From	To	Source	Destination	Schedule	Service	Security Profiles	NAT	Action
sd-wan	Red_Local (port9)	all	Tuvatar Tuvatar 443	always	HTTP ALL_ICMP HTTPS		Enabled	ACCEPT
sd-wan	Red_Local (port9)	all	Publicacion_ministries1	always	HTTP ALL_ICMP HTTPS		Enabled	ACCEPT
sd-wan	Red_Local (port9)	all	Publicacion_Programa	always	HTTP ALL_ICMP HTTPS		Enabled	ACCEPT
sd-wan	Red_Local (port9)	all	Firetst	always	HTTP ALL_ICMP HTTPS		Enabled	ACCEPT
Canal 22 (canal22)	sd-wan	172.31.227.0/24	www.centroculturadigital.mx	always	ALL		Enabled	ACCEPT
Eventos_Canal22 (canal22_eventos)	sd-wan	172.31.228.0/24	all	always	ALL		Enabled	ACCEPT
Eventos_Canal22 (canal22_eventos)	sd-wan	172.31.228.0-24	www.centroculturadigital.mx	always	ALL		Enabled	ACCEPT
TVmetro_Invitados (invitados)	sd-wan	172.31.224.0/24	all	always	ALL		Enabled	ACCEPT
TVmetro_Invitados (invitados)	sd-wan	172.31.224.0/24	www.centroculturadigital.mx	always	ALL		Enabled	ACCEPT

From	To	Source	Destination	Schedule	Service	Security Profiles	NAT	Action
Red_Local (port7)	sd-wan	10.252.10.0/26 172.16.1.0/24 172.20.22.0/26 172.31.215.0/24 192.168.0.0/16 192.168.122.0/24 10.0.0.252 VAF	www.centroculturadigital.mx	always	ALL		Enabled	ACCEPT
Red_Local (port7)	sd-wan	172.16.1.0/24	all	always	ALL		Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.31.215.0/24	all	always	ALL		Enabled	ACCEPT
Red_Local (port7)	sd-wan	172.20.22.10/32	all	always	ALL		Enabled	ACCEPT
Red_Local (port7)	sd-wan	172.20.22.15 correo	all	always	ALL		Enabled	ACCEPT
Red_Local (port7)	sd-wan	172.20.21.0-26	all	always	ALL		Enabled	ACCEPT
Red_Local (port9)	sd-wan	10.252.10.0/26	all	always	ALL		Enabled	ACCEPT

From	To	Source	Destination	Schedule	Service	Security Profiles	NAT	Action
Red_Local (port9)	sd-wan	172.20.222.0/26 172.31.213.0/24 192.168.0.0/16 192.168.222.0/24 10.0.0.252_WAF	all	always	ALL	[redacted]	Enabled	ACCEPT
Red_Local (port9)	sd-wan	10.0.0.0/24	all	always	ALL	[redacted]	Enabled	ACCEPT
CENAM	Red_Local (port9)	192.168.0.13/32 192.168.0.33/32 192.168.0.120/32	10.0.0.252_WAF	always	ALL_ICMP ALL_UDP		Enabled	ACCEPT
CENAM	Red_Local (port9)	192.168.0.13/32 192.168.0.32/32 192.168.0.120/32	10.0.0.254/32	always	ALL_ICMP ALL_UDP		Disabled	ACCEPT
Red_Local (port9)	CENAM	10.0.0.254/32 10.0.0.252_WAF	192.168.0.13/32	always	ALL_ICMP ALL_UDP		Disabled	ACCEPT
GW-CAN22-INFAG	Red_Local (port9)	192.168.129.192/27 192.168.142.0/24	10.0.0.252_WAF 10.0.0.254/32	always	ALL_ICMP HTTP HTTPS SSH SNMP		Disabled	ACCEPT
GW-CAN22-INFAG	Red_Local (port9)	192.168.120.128/32_FORTIANALYZER	10.0.0.254/32	always	ALL		Disabled	ACCEPT
Red_Local (port9)	GW-CAN22-INFAG	10.0.0.252_WAF 10.0.0.254/32	192.168.129.220/32_MonitoreoSOC 192.168.129.219/32_Monitoreo2	always	ALL_ICMP SNMP		Disabled	ACCEPT
Red_Local (port9)	GW-CAN22-INFAG	10.0.0.254/32	192.168.120.129/32_FORTIMANAGER	always	ALL		Disabled	ACCEPT
GW-CAN22-INFAG	Red_Local (port9)	192.168.120.129/32_FORTIMANAGER	10.0.0.254/32	always	ALL		Disabled	ACCEPT

From	To	Source	Destination	Schedule	Service	Security Profiles	NAT	Action
Red_Local (port9)	GW-CANAL-PRESI	10.0.0.254/32	172.18.121.105/32_Zabbix	always	SNMP ALL_ICMP		Disabled	ACCEPT
sd-wan	Red_Local (port9)	all	MTP-189.204.131.152-10.252.10.3	always	FTP SSH		Disabled	ACCEPT
sd-wan	Red_Local (port9)	all	Portal Transparencia_80 Portal Transparencia_443	always	HTTP HTTPS		Disabled	ACCEPT
GW-CNL_INFOSF	Red_Local (port9)	192.168.86.0/24	10.0.0.0/24	always	ALL		Disabled	ACCEPT
GW-CNL_INFOSF	Red_Local (port9)	192.168.110.64/26	10.0.0.211/32	always	ALL		Disabled	ACCEPT
GW-C22-INF-AGS	Red_Local (port9)	172.22.223.65/32	10.0.0.252_WAF 10.0.0.254/32	always	SNMP ALL_ICMP		Disabled	ACCEPT
GW-CANAL-VPNAGS	Red_Local (port9)	RED_VPN_SEG	10.0.0.0/24	always	ALL		Disabled	ACCEPT
GW-CANAL-PRESI	Red_Local (port9)	172.18.121.101/32_Monitoreo	10.0.0.252_WAF 10.0.0.254/32	always	ALL_ICMP SNMP		Disabled	ACCEPT
GW-CANAL-PRESI	Red_Local (port9)	172.18.121.115/32	10.0.0.252_WAF 10.0.0.254/32	always	ALL_ICMP SSH		Disabled	ACCEPT
Red_Local (port9)	GW-CANAL-VPNAGS	10.0.0.254/32 10.0.0.252_WAF	172.22.18.193/32_FAZ	always	FortiAnalyzer PING		Disabled	ACCEPT
GW-CANAL-VPNAGS	Red_Local (port9)	172.22.77.1/32_Monitoreo	10.0.0.252_WAF 10.0.0.254/32	always	ALL_ICMP SNMP		Disabled	ACCEPT
GW-CNL_INFOSF	Red_Local (port9)	192.168.97.10/32_monitoreo	10.0.0.252_WAF 10.0.0.254/32	always	ALL_ICMP SNMP		Disabled	ACCEPT

From	To	Source	Destination	Schedule	Service	Security Profiles	NAT	Action
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 daniela abigail claudia jose	172.20.22.44/32 172.20.22.46/32 172.20.22.35/32 172.20.22.12/32 172.20.22.43/32	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 daniela	172.20.22.10/32 172.20.22.44/32 172.20.22.46/32 172.20.22.35/32 172.31.220.43/32_Sin restricciones	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 erika	172.16.1.245/32	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 guillermo	172.16.1.107/32	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 anayeli	172.20.22.50/32 172.20.22.54/32 172.20.22.58/32	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 hugo juan alfredo gbac	172.16.0.0/12	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 gbac	172.31.213.0/24 100.0.1-100.0.251	always	ALL		Disabled	ACCEPT
Red_Local (port9)	sd-wan	172.31.200.0/23	all	always	ALL		Enabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 claudialuna	172.31.220.6/32	always	ALL		Disabled	ACCEPT
Canal 22 (canal22)	Red_Local (port9)	172.31.227.0/24	10.100.10.0/24 10.252.10.0/26 172.16.1.0/24 172.20.22.0/26 172.31.215.0/24 172.31.221.0/24 192.168.0.0/16 172.31.200.0/23	always	ALL		Disabled	ACCEPT
Red_Local (port9)	Canal 22 (canal22)	10.100.10.0/24 10.252.10.0/26 172.16.1.0/24 172.20.22.0/26 172.31.200.0/23 172.31.215.0/24 172.31.221.0/24 192.168.0.0/16	172.31.227.0/24	always	ALL		Disabled	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 (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

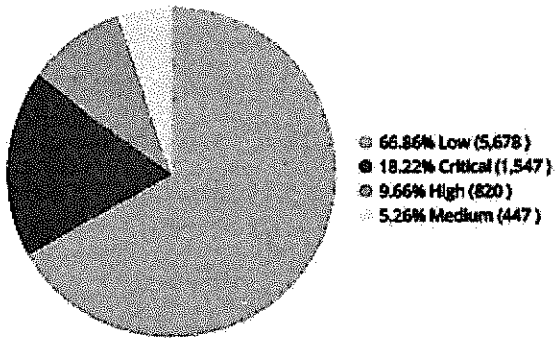
Name	Severity	Target	OS
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS		Server	Linux
3Com.OfficeConnect.Utility.CGI.Remote.Command.Execution		Server	Linux
7-Zip.RAR.Solid.Compression.Remote.Code.Execution		Server, Client	Windows
427BB.Cookie.Based.Authentication.Bypass		Server	Other
Aardvark.Topsites.PHP.Remote.Command.Execution		Server	Windows, Linux, BSD, Solaris, MacOS
ABBS.Audio.Media.Player.LST.Buffer.Overflow		Server, Client	Windows
ACal.Calendar.Cookie.Based.Authentication.Bypass		Server	Windows, Linux, BSD, Solaris, MacOS
Accellion.FTA.auth_params.CRLF.Injection		Server	Linux, BSD
Accellion.FTA.Cookie.Information.Disclosure		Server	Linux, BSD
Accellion.FTA.display.parameter.CRLF.Injection		Server	Linux, BSD
Accellion.FTA.getStatus.verify_oauth_token.Command.Injection		Server	Linux, BSD
Accellion.FTA.LDAP.Injection		Server	Linux, BSD
Accellion.FTA.wmProgressval.SSRF		Server	Linux, BSD
ACME.mini_httpd.Arbitrary.File.Read		Server	Linux
Acrobat.Acrobat.Reader.CVE-2020-24434.Out.of.Bounds.Read		Server, Client	Windows, MacOS
Acrobat.Reader.Acrobat.CVE-2020-24433.Arbitrary.File.Creation		Server, Client	Windows, MacOS
ActivePDF.Toolkit.Multiple.File.Memory.Corruption		Server, Client	Windows
ActivePerl.PerlIS.dll.Remote.Buffer.Overflow		Server	Windows

« ‹ 1 /61 › » [Total: 3010]

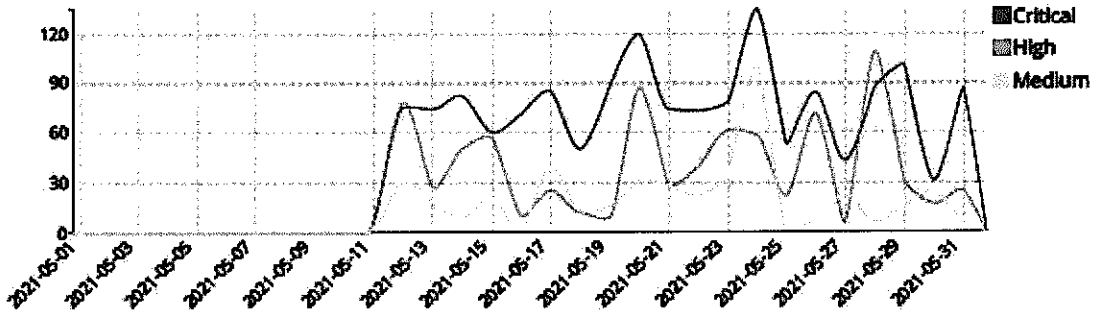
3.1. Ataques detectados y detenidos por el IPS

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	572
2	ThinkPHP.Controller.Parameter.Remote.Code.Execution	CVE-2019-9082,CVE-2018-20062	Code Injection	206
3	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	CVE-2015-2051,CVE-2019-10891	OS Command Injection	189
4	Dasan.GPON.Remote.Code.Execution	CVE-2018-10561,CVE-2018-10562	OS Command Injection	153
5	Zeroshell.Kerbynet.Type.Parameter.Remote.Command.Execution	CVE-2009-0545,CVE-2019-12725	Code Injection	81
6	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	CVE-2017-5638	Code Injection	56
7	Joomla!.Core.Session.Remote.Code.Execution	CVE-2015-8562	Code Injection	54
8	vBulletin.Routestring.widgetConfig.Remote.Code.Execution	CVE-2019-16759	Code Injection	51
9	WordPress.HTTP.Path.Traversal	CVE-2019-9618,CVE-2018-16283,CVE-2018-16299,CVE-2020-11738	Path Traversal	34
10	vBulletin.tabbedcontainer.Template.Remote.PHP.Code.Execution	CVE-2020-7373,CVE-2020-17496	Code Injection	31
11	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution		Code Injection	30
12	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	CVE-2017-11317,CVE-2017-11357,CVE-2019-18935	Improper Authentication	16
13	Shenzhen.TVT.DVR.Remote.Code.Execution		Permission/Priviledge/Access Control	13
14	Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	CVE-2018-7600	OS Command Injection	12
15	Gozi.Botnet			10
16	HTTP.URI.Java.Code.Injection	CVE-2018-1273	Code Injection	7
17	BuilderEngine.elFinder.Arbitrary.File.Upload		Permission/Priviledge/Access Control	6
18	Red.Hat.JBoss.AS.doFilter.Insecure.Deserialization	CVE-2017-12149	OS Command Injection	5
19	Bladabindi.Botnet			5
20	Gh0st.Rat.Botnet			4

High Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	ELFinder.Connector.Mkfile.php.Arbitrary.File.Upload	CVE-2020-25213	Permission/Privilege/Access Control	241
2	Mirai.Botnet			169
3	HTTP.URI.SQL.Injection		SQL Injection	121
4	JAWS.DVR.CCTV.Shell.Unauthenticated.Command.Execution		OS Command Injection	101
5	PHP.CGI.Argument.Injection	CVE-2012-1823,CVE-2012-2311	Code Injection	51
6	PhpStudy.Web.Server.Remote.Code.Execution		Code Injection	34
7	ThinkPHP.Request.Method.Remote.Code.Execution		Code Injection	24
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-2021-29447	Other	19
9	Axis.SSI.cambr.Remote.Command.Execution		Code Injection	13
10	ThinkPHP.HTTP.VARS.S.Remote.Code.Injection		Code Injection	9
11	Tongda.Office.Anywhere.Unauthorized.File.Upload		Improper Authentication	9
12	Seeyon.Office.Anywhere.htmlofficeservlet.Arbitrary.File.Upload		OS Command Injection	8
13	HTTP.Header.SQL.Injection		SQL Injection	6
14	Tomato.Router.Default.Credentials		Anomaly	6
15	China.Chopper.Web.Shell.Client.Connection		Anomaly	3
16	Nedrix.GPON.Router.formPing.Remote.Command.Injection		OS Command Injection	1
17	HTTP.Unix.Shell.LFS.Remote.Code.Execution		OS Command Injection	1
18	PHP.Malicious.Shell		Malware	1
19	D-Link.DSL.2640B.Unauthenticated.DNS.Change.Policy.Bypass		Improper Authentication	1

Medium Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	Web.Server.Password.Files.Access		Permission/Priviledge/Access Control	226
2	PHP.Diescan		Anomaly	122
3	WordPress.xmlrpc.php.system.multicall.Amplification.Attack		Anomaly	49
4	WordPress.REST.API.Username.Enumeration.Information.Disclosure	CVE-2017-5487	Information Disclosure	19
5	FCKeditor.CurrentFolder.Arbitrary.File.Upload	CVE-2009-2265	Permission/Priviledge/Access Control	11
6	Phpweb.CMS.appcode.Information.Disclosure		Information Disclosure	8
7	HTTP.Referer.Header.SQL.Injection	CVE-2007-1061	SQL Injection	6
8	Apache.Axis2.Default.Password.Access	CVE-2010-0219	Other	6

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	572
2	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Critical	206
3	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	Critical	189
4	Gaisan.GPON.Remote.Code.Execution	Critical	130
5	Zeroshell.Kerbynet.Type.Parameter.Remote.Command.Execution	Critical	81
6	Joomla!.Core.Session.Remote.Code.Execution	Critical	54
7	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Critical	52
8	vBulletin.Routestring.widgetConfig.Remote.Code.Execution	Critical	51
9	WordPress.HTTP.Path.Traversal	Critical	34
10	vBulletin.tabbedcontainer.Template.Remote.PHP.Code.Execution	Critical	31
11	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Critical	16
12	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Critical	15
13	Shenzhen.TVT.DVR.Remote.Code.Execution	Critical	13
14	Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	Critical	12
15	Gozi.Botnet	Critical	10
16	BuilderEngine.elFinder.Arbitrary.File.Upload	Critical	6
17	Bladabindi.Botnet	Critical	5
18	Linux.Kernel.TCP.SACK.Panic.DoS	Critical	4
19	GhOst.Rat.Botnet	Critical	4

https://fortiguard.com/encyclopedia/ips/40772

20	TerraMaster.TOS.Makecvs.PHP.Unauthenticated.Command.Execution	Critical		2
21	MikroTik.RouterOS.Arbitrary.File.Read	Critical		2
22	Red.Hat.JBoss.AS.doFilter.Insecure.Deserialization	Critical		2
23	Bash.Function.Definitions.Remote.Code.Execution	Critical		1
24	F5.BIG.IP.Traffic.Management.User.Interface.Directory.Traversal	Critical		1
25	D-Link.DSL-2750B.CLI.OS.Command.Injection	Critical		1
26	ELFinder.Connector.Minimal.php.Arbitrary.File.Upload	High		241
27	Mirai.Botnet	High		169
28	HTTP.URI.SQL.Injection	High		121
29	JAWS.DVR.CCTV.Shell.Unauthenticated.Command.Execution	High		99
30	PHP.CGI.Argument.Injection	High		51
31	PhpStudy.Web.Server.Remote.Code.Execution	High		34
32	ThinkPHP.Request.Method.Remote.Code.Execution	High		24
33	Generic.XXE.Detection	High		19
34	Axis.SSI.camnbr.Remote.Command.Execution	High		12
35	Tongda.Office.Anywhere.Unauthorized.File.Upload	High		9
36	ThinkPHP.HTTP.VARS.S.Remote.Code.Injection	High		9
37	Seeyon.Office.Anywhere.htmlofficeservlet.Arbitrary.File.Upload	High		8
38	HTTP.Header.SQL.Injection	High		6
39	China.Chopper.Web.Shell.Client.Connection	High		3
40	HTTP.Unix.Shell.IFS.Remote.Code.Execution	High		1
41	D-Link.DSL.2640B.Unauthenticated.DNS.Change.Policy.Bypass	High		1
42	Netlink.GPON.Router.formPing.Remote.Command.Injection	High		1
43	Zyxel.Cloud.CNM.SecuManager.Remote.Command.Execution	High		1
44	PHP.Malicious.Shell	High		1
45	Web.Server.Password.Files.Access	Medium		226
46	PHP.Diescan	Medium		122
47	WordPress.xmlrpc.php.system.multicall.Amplification.Attack	Medium		49
48	WordPress.REST.API.Username.Enumeration.Information.Disclosure	Medium		19

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	172.20.22.44				822	29.21%
2	10.0.0.208				278	9.88%
3	10.0.0.202				251	8.92%
4	172.20.22.25				227	8.07%
5	172.20.22.11				221	7.85%
6	10.0.0.216				190	6.75%
7	172.20.22.18				177	6.29%
8	10.252.10.20				145	5.15%
9	10.0.0.207				136	4.83%
10	10.0.0.211				134	4.76%
11	172.20.22.35				132	4.69%
12	10.0.0.209				101	3.59%

Intrusion Sources

#	Attack Source	Counts	Critical	High	Medium	Percent of Total Attacks
1	45.146.164.125				294	20.75%
2	189.203.227.34				247	17.43%
3	45.155.205.181				164	11.57%
4	209.141.33.232				97	6.85%
5	180.76.143.249				51	3.60%
6	180.215.229.158				50	3.53%
7	182.75.35.100				50	3.53%
8	62.183.2.190				49	3.46%
9	112.53.100.233				45	3.18%
10	27.124.2.27				44	3.11%
11	45.155.205.125				43	3.03%
12	45.146.164.152				43	3.03%
13	47.101.220.233				38	2.68%
14	45.155.205.109				31	2.19%
15	187.190.11.140				30	2.12%
16	45.155.205.196				30	2.12%
17	5.188.84.19				29	2.05%
18	216.4.95.62				28	1.98%
19	156.200.107.244				28	1.98%
20	203.177.140.42				26	1.83%

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		572
2	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Code Injection	Critical		206
3	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	Critical		189
4	Dasan.GPON.Remote.Code.Execution	OS Command Injection	Critical		153
5	Zeroshell.Kerbynet.Type.Parameter.Remote.Command.Execution	Code Injection	Critical		81
6	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Code Injection	Critical		56
7	Joomla!.Core.Session.Remote.Code.Execution	Code Injection	Critical		54
8	vBulletin.Routestring.widgetConfig.Remote.Code.Execution	Code Injection	Critical		51
9	WordPress.HTTP.Path.Traversal	Path Traversal	Critical		34
10	vBulletin.tabbedcontainer.Template.Remote.PHP.Code.Execution	Code Injection	Critical		31
11	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection	Critical		30
12	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Improper Authentication	Critical		16
13	Shenzhen.TVT.DVR.Remote.Code.Execution	Permission/Priviledge/Access Control	Critical		13
14	Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	OS Command Injection	Critical		12

3.4. Tipo y número de ataques detectados y detenidos

Intrusions By Types

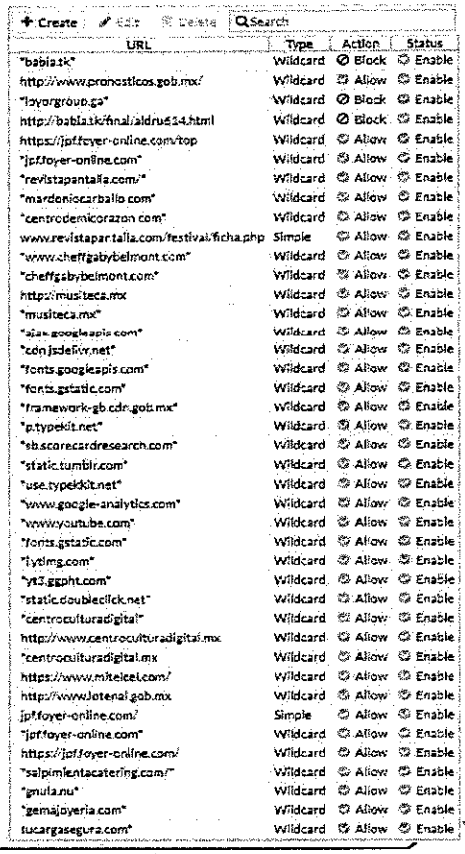
#	Intrusion Type	Counts
1	Anomaly	5,715
2	Code Injection	1,219
3	Permission/Priviledge/Access Control	498
4	OS Command Injection	475
5	Malware	144
6	SQL Injection	133
7	Path Traversal	38
8	Information Disclosure	27
9	Improper Authentication	26
10	Other	25
11	DoS	4

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 New | Edit | Delete

Pattern Type	Pattern	Language	Action	Status
Wildcard	http://babla.tk/final/aldru614.html	Western	Block	Enable
Wildcard	"babla.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



+ Create | Edit | Delete | Search

URL	Type	Action	Status
"babla.tk"	Wildcard	Block	Enable
http://www.pronosticos.gob.mx/	Wildcard	Allow	Enable
"foyergroup.ga"	Wildcard	Block	Enable
http://babla.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
"mardonicarballo.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
"tvdmg.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.miteleel.com/	Wildcard	Allow	Enable
http://www.lotenal.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	29,895

5. Direcciones ip con mayor consumo de ancho de banda

Top 20 Bandwidth Users

#	User (or IP)	Bandwidth
1	10.100.1.231	142.91 GB
2	172.31.226.9	24.31 GB
3	172.16.1.6	22.78 GB
4	172.31.215.168	21.81 GB
5	172.31.226.12	19.18 GB
6	172.16.1.153	18.95 GB
7	172.31.228.5	17.65 GB
8	172.31.228.6	16.81 GB
9	172.16.1.61	12.93 GB
10	172.16.1.185	12.48 GB
11	172.31.215.48	12.41 GB
12	172.16.1.245	11.65 GB
13	172.16.1.136	11.15 GB
14	172.16.1.108	10.59 GB
15	172.16.1.236	10.13 GB
16	172.16.1.1	10.12 GB
17	172.31.226.24	9.79 GB
18	172.31.226.77	9.53 GB
19	172.16.1.219	9.31 GB
20	172.31.226.13	8.03 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		477.44 GB		87,929
2	172.31.201.25		471.81 GB		19,092
3	172.31.200.72		469.41 GB		28,627
4	172.31.201.64		375.20 GB		1,249,478
5	172.31.201.205		337.69 GB		341,474
6	10.252.10.8		254.58 GB		546
7	10.252.10.7		215.70 GB		583
8	10.100.1.231		209.26 GB		377,167
9	172.20.22.19		159.23 GB		67,865,775
10	172.31.200.154		158.91 GB		426,521
11	172.31.201.17		118.98 GB		12,438
12	172.31.215.168		83.92 GB		126,658
13	172.31.200.171		82.09 GB		140,456
14	172.31.200.104		72.47 GB		66,863
15	172.31.200.70		70.56 GB		44,308
16	172.31.200.139		64.47 GB		2,807,601
17	172.31.201.246		57.11 GB		51,498
18	172.31.226.99		56.87 GB		19,406
19	172.31.200.250		55.18 GB		221,677
20	172.31.201.204		54.05 GB		100,881
21	172.31.201.235		52.52 GB		111,095
22	172.16.1.153		51.37 GB		244,476
23	172.31.201.120		50.25 GB		11,331
24	172.31.200.30		47.45 GB		85,484
25	172.31.226.9		44.98 GB		97,884
26	172.31.200.123		44.89 GB		93,062
27	172.31.201.39		42.60 GB		161,961
28	172.31.200.218		41.86 GB		74,911
29	172.31.200.56		36.47 GB		20,733
30	172.31.226.12		35.64 GB		103,341

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		746.77 GB
2	Web.Client		636.88 GB
3	Social.Media		282.58 GB
4	Email		250.22 GB
5	Collaboration		151.59 GB
6	Unknown		79.11 GB
7	General.Interest		72.73 GB
8	Update		63.60 GB
9	Network.Service		36.16 GB
10	Storage.Backup		28.09 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	☑	
16	Subdominios	Subdominios canal22	HTTP	HTTPS	Single Server/Server Pool	Inline Alert Only	Disable	☑	

6.2. Resumen de tipo de ataque.

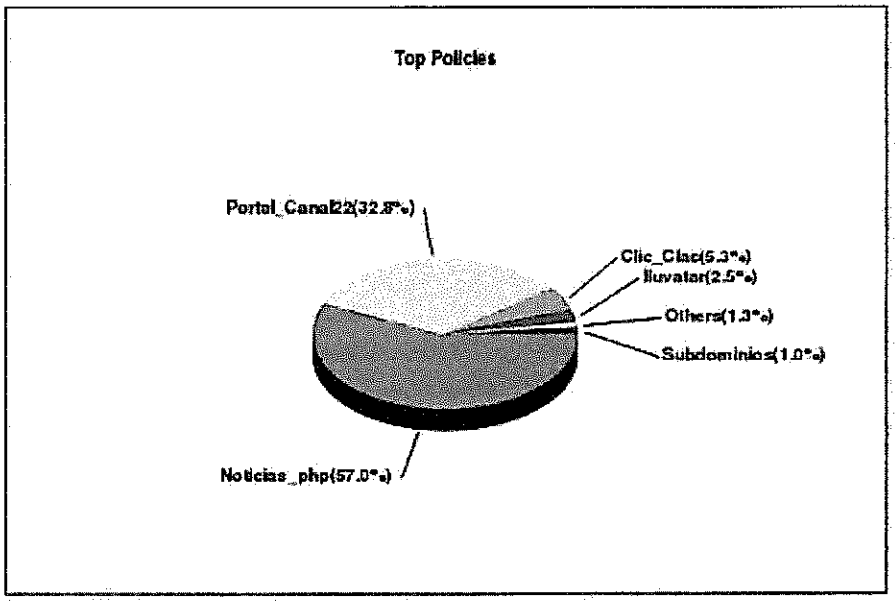
La tabla siguiente muestra un resumen de los ataques detectados y bloqueados por el WAF

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
2021-04-30	Directory Listing	66	63.46
	HTTP Header Leakage	23	22.12
	Bad Robot	3	2.88
	Other(8)	12	11.54
	Subtotal(11)	104	0.07
2021-05-01	Directory Listing	4578	79.85
	HTTP Header Leakage	561	9.79
	RFI Injection	242	4.22
	Other(17)	352	6.14
	Subtotal(20)	5733	3.75
2021-05-02	Directory Listing	1546	58.58
	HTTP Header Leakage	530	20.08
	Malformed Request	164	6.21
	Other(19)	399	15.12
	Subtotal(22)	2639	1.72
2021-05-03	HTTP Header Leakage	2659	49.20
	Directory Listing	2300	42.55
	Malformed Request	127	2.35
	Other(21)	319	5.90
	Subtotal(24)	5405	3.53
2021-05-04	Directory Listing	4067	68.01
	HTTP Header Leakage	1376	23.01
	Bad Robot	156	2.61
	Other(21)	381	6.37
	Subtotal(24)	5980	3.91
2021-05-05	Directory Listing	2910	57.46
	HTTP Header Leakage	1752	34.60
	Bad Robot	130	2.57
	Other(16)	272	5.37
	Subtotal(19)	5064	3.31
Other(26)		128064	83.71
Total(32)		**152989**	**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	85368	55.80
/cartelera/backend/application.php	19794	12.94
/	16314	10.66
/wp-login.php	3075	2.01
none	3063	2.00
/ap/uedata	2650	1.73
Other(7521)	22725	14.85
Total(7527)	**152989**	**100.00**