



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

N° de Solicitud		
FECHA DE RECEPCIÓN		
DIA	MES	AÑO

SOLICITUD DE PAGO

ÁREA SOLICITANTE: GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN
 CENTRO DE COSTO: VARIOS REQUISICIÓN No.: 300
 CONTRATO No.: 6/6/2021
 FORMA DE ADJUDICACIÓN: FACTURA No.: F19818
 No. SICOP: 016674
 DIRECTA: INVITACIÓN: LICITACIÓN: EXCEPCIÓN ART.41

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

IMPORTE: \$209,446.27
 DOSCIENTOS NUEVE MIL CUATROCIENTOS CUARENTA Y SEIS PESOS 27 /100 MN)

DESCRIPCIÓN DEL BIEN O SERVICIO: Enlace Dedicado a Internet de 200 Mbps o superior, Suministro y operación de equipamiento de Seguridad Perimetral WAN (UTM), Suministro y operación de equipamiento de Acceso Seguro WLAN y WIFI, Suministro y operación de equipamiento de Seguridad para Servidores Web (WAF). Correspondiente al mes de agosto 2021.

Transferencia Bancaria: **CLABE:** 012180001540457774
Banco: BBVA Bancomer, S.A.
Cuenta: 0154045777

PARA USO EXCLUSIVO DE LA DIRECCIÓN DE FINANZAS

GERENCIA DE PRESUPUESTO

DEPTO. DE TESORERÍA

PRE PROCESO:	
PRE SUF:	
COM. PROCESO	
COMPROMISO	

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

CADENAS PRODUCTIVAS

CLAVE DE AFECTACIÓN PRESUPUESTAL RUBRICA

PARTIDA: _____ C.C. _____ FF: _____

VISTO BUENO DE CONTABILIDAD RUBRICA

NOMBRE: _____

NOMBRE: _____

ÁREA RESPONSABLE DEL GASTO:

AUTORIZA:



 ING. JUAN PABLO ROSAS TURANZAS
 GERENTE DE TECNOLOGÍAS DE LA INFORMACIÓN

 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: Enlace Dedicado a Internet de 200 Mbps o superior, Suministro y operación de equipamiento de Seguridad Perimetral WAN (UTM), Suministro y operación de equipamiento de Acceso Seguro WLAN y WIFI, Suministro y operación de equipamiento de Seguridad para Servidores Web (WAF).
Correspondiente al mes de agosto 2021.

FECHA DE RECEPCIÓN: AGOSTO 2021

No. DE CONTRATO: 6/6/2021
No. DE REQUISICIÓN: 300

No. DE FACTURA:
F19818

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 19818

Folio Fiscal AAFE2F45-6431-404F-A2F8-1300721B4642
Fecha Emisión 2021-09-10T00:00:00
Fecha Certificación 2021-09-10T17:31:35
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 21421289/TME
Atención Ing. Juan Pablo Rosas Turanzas
Puesto Gerencia en Tecnologías de la Información

Cantidad	Clave	Descripción	Unidad	Precio Unitario	Importe	
1.00	81141902	Enlace Dedicado a Internet de 200 Mbps o superior	ACT	26,682.35	26,682.35	
		Impuesto	Tipo	Tasa	Base	Importe
		Traslado	002	Tasa	0.160000	26,682.35
1.00	81141902	Suministro y operación de equipamiento de Seguridad Perimetral WAN (UTM)	E48	53,593.87	53,593.87	
		Impuesto	Tipo	Tasa	Base	Importe
		Traslado	002	Tasa	0.160000	53,593.87
1.00	81141902	Suministro y operación de equipamiento de Acceso Seguro WLAN y WIFI	E48	54,131.48	54,131.48	
		Impuesto	Tipo	Tasa	Base	Importe
		Traslado	002	Tasa	0.160000	54,131.48
1.00	81141902	Suministro y operación de equipamiento de Seguridad para Servidores Web (WAF)	E48	46,149.42	46,149.42	
		Impuesto	Tipo	Tasa	Base	Importe
		Traslado	002	Tasa	0.160000	46,149.42
		Impuesto	Tipo	Tasa	Base	Importe
		Traslado	002	Tasa	0.160000	7,383.91

SERVICIOS CORRESPONDIENTES AL PERIODO DEL MES DE AGOSTO DE 2021

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

Subtotal 180,557.12
IVA 16.00% 28,889.15
Total 209,446.27

Cantidad con Letra: (DOSCIENTOS NUEVE MIL CUATROCIENTOS CUARENTA Y SEIS PESOS 27/100 M.N.)



Sello digital del CFDI

FyFTCcacd2FlaEjOllz8AOWJL4wfrPV0a5BQa4NGIpfw8s1+wTxo1W/IQ770ZwXqW0PqBu8xisUKPuHZO7gUSNz5PcfEYALhQ9t1/axkLSRRXMJ2CqC17MZIDB6LTwt9I3B7ETAo3aHXwNqHbzleUZqkMOd+Drq0YddlenMmmZbvQaazoOIMp1oSfAQdPZ3j5g9IVPY3M3Q48k6RNqvF5EVrNk+qeVGpnUlw6BCHvWTR1/KVJhV3j1h2EILqX23KJ1LuFw6GnLbIug5EQnqM84EkoDdfRrcJJTB4b9jHDh9U6amoRLkp6NYSqdsFVhesJhizqzinqSQ0hgTg==

Sello digital del SAT

kZOGILJOKRv8wSBZNeq6Qhb1s5o5Mme1sDeJigcAWOeH/NuKeM1YnHMaFp077TvTLzyc34TjUJCTXUv8A0RZjtRnAInkT2PPIU//KUH0CIEQv2mhQTvjwuc2TIRzdwq/5aV5GV66VQiIMY0ZBLh89pXFewVVgV1CX83YCxAYSNI5pQ/G6XXjiYFDV+1Z2uVTw/2plyeBavVejXo9UeSg0fR8TKBxf7QLoYFgoHI+qRCGYBh1YzTzB5UAPQ+d4PLypG6WoelroVDLItX4IWRV44gkAFie10HOBHID1DRJJ0kLYWqAWPI38zvKIXhBAIcnQ7n7hXq3u4hZAIw==

Cadena original del complemento de certificación digital del SAT

||1.1|AAFE2F45-6431-404F-A2F8-1300721B4642|2021-09-10T17:31:35|TLE0111225C2|FyFTCcacd2FlaEjOllz8AOWJL4wfrPV0a5BQa4NGIpfw8s1+wTxo1W/IQ770ZwXqW0PqBu8xisUKPuHZO7gUSNz5PcfEYALhQ9t1/axkLSRRXMJ2CqC17MZIDB6LTwt9I3B7ETAo3aHXwNqHbzleUZqkMOd+Drq0YddlenMmmZbvQaazoOIMp1oSfAQdPZ3j5g9IVPY3M3Q48k6RNqvF5EVrNk+qeVGpnUlw6BCHvWTR1/KVJhV3j1h2EILqX23KJ1LuFw6GnLbIug5EQnqM84EkoDdfRrcJJTB4b9jHDh9U6amoRLkp6NYSqdsFVhesJhizqzinqSQ0hgTg==|00001000000503270882||

Recepción de compra

Pág.: 1

Número recepción de compra: RECEP-21-1048
Fecha recepción de compra: 14/09/2021

Compra

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

Enviar
Para:

Envío a través de

Recibir por 10/09/2021
Id. proveedor P01001338

Confirmar a
Comprador
Número pedido C-PED-21-1091
Fecha pedido 14/09/2021

Nº producto	Descripción	Unidad	Recibido	Pedido	Pedido pendiente
	Nº licitación: PC-21-0272				
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	GASTOS DE VENTA	SER	1	1	
	GASTOS DE VENTA	SER	1	1	
	GASTOS DE ADMINISTRACION	SER	1	1	
	GASTOS DE ADMINISTRACION	SER	1	1	
	GASTOS DE ADMINISTRACION	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	GASTOS DE ADMINISTRACION	SER	1	1	
	GASTOS DE ADMINISTRACION	SER	1	1	

Factura compra

Pág.: 1

No. CFACT-21-1048
Número factura compra: F19818
Fecha factura compra: 14/09/2021
Número de evento: EV1-21-000991

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

Enviar
Para:

Tipo de Persona Moral
Envío a través de
Recibir por 10/09/2021
Términos
Id. proveedor P01001338

Confirmar a
Comprador
Número pedido C-PED-21-1091
Fecha pedido 14/09/2021
Forma de pago

Nº producto	PP	PTDA ESP	FF	CECO	Descripción	Unidad	Cantidad	Precio	Precio total
					Nº licitación: PC-21-0272				
013	31603	1	11		MATERIALES INDIRECTOS	SER	1	4,358.28	4,358.28
013	31603	1	12		MATERIALES INDIRECTOS	SER	1	3,735.66	3,735.66
013	31603	1	13		MATERIALES INDIRECTOS	SER	1	7,471.32	7,471.32
013	31603	1	21		MATERIALES INDIRECTOS	SER	1	4,980.88	4,980.88
013	31603	1	22		MATERIALES INDIRECTOS	SER	1	19,923.52	19,923.52
013	31603	1	23		MATERIALES INDIRECTOS	SER	1	9,961.76	9,961.76
013	31603	1	24		MATERIALES INDIRECTOS	SER	1	9,961.76	9,961.76
013	31603	1	31		GASTOS DE VENTA	SER	1	2,490.44	2,490.44
013	31603	1	32		GASTOS DE VENTA	SER	1	4,358.27	4,358.27
001	31603	1	41		GASTOS DE ADMINISTRACION	SER	1	3,113.05	3,113.05
001	31603	1	42		GASTOS DE ADMINISTRACION	SER	1	31,753.11	31,753.11
001	31603	1	43		GASTOS DE ADMINISTRACION	SER	1	15,565.47	15,565.47
013	31603	1	51		MATERIALES INDIRECTOS	SER	1	6,848.71	6,848.71
013	31603	1	52		MATERIALES INDIRECTOS	SER	1	17,433.08	17,433.08
013	31603	1	53		MATERIALES INDIRECTOS	SER	1	24,904.40	24,904.40
013	31603	1	54		GASTOS DE ADMINISTRACION	SER	1	6,848.71	6,848.71
001	31603	1	61		GASTOS DE ADMINISTRACION	SER	1	6,848.71	6,848.71

Subtotal: 180,557.13
Descuento factura: 0.00
IVA: 28,889.14
Total de MXN: 209,446.27



Autorización de pago

RAUL YAU

No.: SP-21-01452

SUBDIRECTOR GENERAL TECNICO
Y OPERATIVO

No. Autorización: SP-21
-01452

Presente:

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

Por un importe de: \$209,446.27 (DOSCIENTOS NUEVE MIL CUATROCIENTOS CUARENTA Y SEIS PESOS 27/100 M.N.)

Por el pago que se indica en la Solicitud de Pago número SP-21-01452

Recibida con fecha: martes, 14 de septiembre de 2021

Descripción	Importe	No. evento
Servicio de Internet de 200 mbps o superior, Segur	209,446.27	EV1-21-000991
Total:	209,446.27	

Cheque/Transferencia				Beneficiario	Importe
Número	Fecha	Cuenta	No. de póliza	INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	
				Total:	209,446.27

Observaciones: Enlace Dedicado a Internet de 200 Mbps o superior, Suministro y operación de equipamiento de Seguridad Perimetral WAN (UTM), Suministro y operación de equipamiento de Acceso Seguro WLAN y WIFI, Suministro y operación... AGOSTO 2021.

CONSTANCIA DE ENTREGA



SERVICIOS ADMINISTRADOS
AGOSTO 2021

TELEVISIÓN METROPOLITANA, S.A. DE C.V. "CANAL 22"
SERVICIO DE INTERNET DE 200 MBPS O SUPERIOR,
SEGURIDAD PERIMETRAL Y RED WIFI

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







CONSTANCIA DE ENTREGA

Servicio de Internet de 200 Mbps o Superior, Seguridad Perimetral y Red Wifi

Entregables correspondiente al mes de agosto de 2021

Fecha de entrega: 07/09/2021

Servicio	Documento/Archivo	Hash SHA-256	Medio
Reporte de Seguridad Perimetral	E01 - REPORTE DE SEGURIDAD PERIMETRAL AGOSTO 2021 v2.0.pdf	a94195b8c1875155aae0b304b385f4944297730489b19e704b3ede4f480209b3	Electrónico
Reporte de Acceso y Publicación a Internet	E02 - REPORTE DE ACCESO A INTERNET AGOSTO 2021_v2.0.pdf	a12911da6a561a33e4d7d1a6231446a0ead71b5576b2f3ff427db2927277ea6c	
Reporte de Incidentes y Tickets Generados	E03 - REPORTE DE INCIDENTES, REQUERIMIENTOS Y SEGUIMIENTO AGOSTO_v2.0.pdf	d15b1e4e0f1cdf57f5b3cf02e67a2c7304cb944ce1292b53848782e50e80f389	

Clave del entregable	Responsable	Validó	Aprobó
E01 - REPORTE DE SEGURIDAD PERIMETRAL	Rubén Darío Sarmiento Gómez	Eduardo Flores Calderón	Ing. Juan Pablo Rosas Turanzas
E02 - REPORTE DE ACCESO A INTERNET	Encargado de la Gerencia de Administración Integral e Infraestructura	Encargado de Centro de Operaciones de Seguridad	Gerente de Tecnologías de la Información
E03 - REPORTE DE INCIDENTES, REQUERIMIENTOS Y SEGUIMIENTO	Firma	Firma	Firma
			
	Firma	Firma	Firma
			

ANEXOS: 1 CD



Reporte de Seguridad Perimetral

Televisión Metropolitana, S.A. de C.V. “Canal 22”

AGOSTO 2021

Información general del documento

Entregable	Clave	Servicio	Medio
	E01 - SP	Reporte de Seguridad Perimetral	Electrónico

Elaboración	Puesto	Nombre
	Responsable del Servicio	Eduardo Flores Calderón

Revisión	Puesto	Nombre
	Líder de Proyecto	Víctor Quiroz Barrientos

Aprobación	Puesto	Nombre
	Encargado de la Gerencia de Administración Integral e Infraestructura	Rubén Darío Sarmiento Gómez

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

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

Tabla de contenido

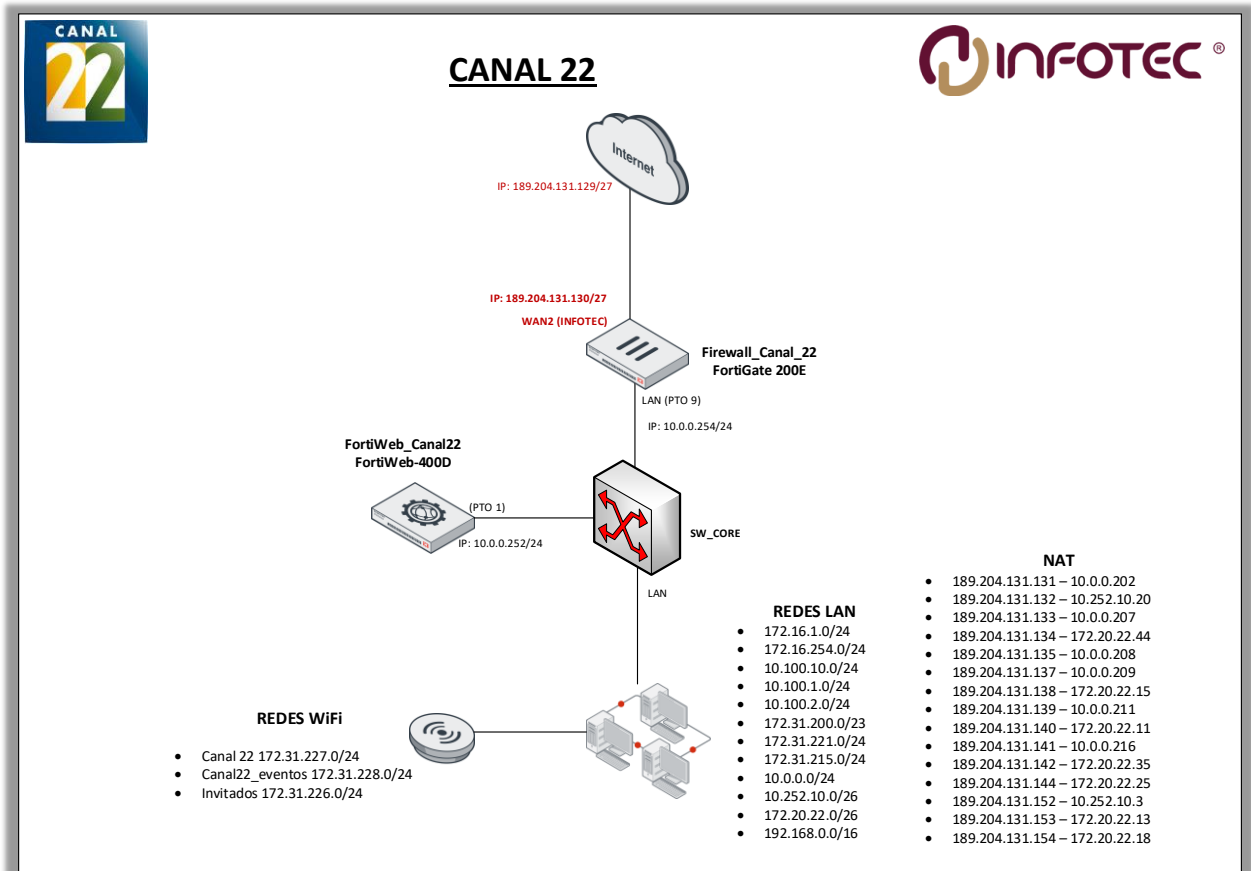
1. Introducción	4
2. Diagrama del Servicio	4
3. Reporte de Firewall de Aplicaciones.....	5
3.1. Políticas aplicadas por mes.....	5
4. Top 10 de Firmas activadas por IPS por mes.....	8
5. Top 10 de IPS con mayor consumo de Internet por mes	9
6. Detalle de los ataques detectados y detenidos	10
7. Reporte de FireWall de Aplicaciones	13
7.1. Incidentes detectados y contenidos por mes	13
8. Tipo y número de ataques detectados y detenidos.....	14
8.1. Top 10 de URLs utilizadas por mes	14
9. Bloqueo de usuarios por URL	16
10. Top 10 de IPS con mayor consumo de ancho de banda.....	16
11. Reporte de Acceso y Publicación a Internet.....	17
12. Consumo de ancho de banda por aplicaciones	18
13. Consumo de usuarios de VPN	18

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. Reporte de Firewall de Aplicaciones

3.1. Políticas aplicadas por mes

En el mes de agosto 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	Action	NAT
Red_Local (port9)	sd-wan	172.31.220.1/32_Emlilio	all	always	ALL		ACCEPT	Enabled
Red_Local (port9)	sd-wan	172.31.220.124/32 172.31.210.100/32	all	always	ALL		ACCEPT	@ 189.240.110.185_Niba
Red_Local (port9)	sd-wan	10.100.10.34-10.100.10.43	www.adobe.com adobe.net adobe.io adobe.com.mx adobe.com* 4.2.2.1_DNS	always	ALL	WEB APP SSL	ACCEPT	Enabled
Red_Local (port9)	sd-wan	10.100.10.34-10.100.10.43	all	always	ALL		DENY	
Red_Local (port9)	sd-wan	172.16.1.0/24 10.100.10.0/24	all	always	ALL	AV WEB APP SSL	ACCEPT	Enabled
Red_Local (port9)	sd-wan	10.100.1.0/24 10.100.2.0/24	all	always	ALL	AV WEB APP SSL	ACCEPT	Enabled
Red_Local (port9)	sd-wan	172.31.220.241-172.31.220.248	all	always	ALL	WEB APP SSL	ACCEPT	Enabled
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	ACCEPT	Enabled
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	ACCEPT	@ segmento 172.31.215.0
Red_Local (port9)	sd-wan	172.31.210.33	all	always	ALL	WEB APP SSL	ACCEPT	Enabled
Red_Local (port9)	sd-wan	172.31.210.33	all	always	ALL	WEB APP SSL	ACCEPT	@ segmento 172.31.210.0
Red_Local (port9)	sd-wan	172.31.210.18/32 172.31.210.188/32	all	always	ALL	WEB APP SSL	ACCEPT	Enabled
Red_Local (port9)	sd-wan	172.31.210.18/32 172.31.210.188/32	all	always	ALL	WEB APP SSL	ACCEPT	@ segmento 172.31.210.0
Canal 22 (canal22)	sd-wan	172.31.227.0/24	all	always	ALL	WEB APP SSL	ACCEPT	Enabled
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		ACCEPT	Disabled
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		ACCEPT	Disabled
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		ACCEPT	Disabled
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 angelica.aguirre ev4.arellano rodrigo.moctezuma	10.100.10.20/32	always	ALL		ACCEPT	Disabled
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		ACCEPT	Disabled

sd-wan	Red_Local (port9)	all	Portal Proyectos Portal Proyectos_443	always	ALL_ICMP HTTP HTTPS	IPS SSL	ACCEPT	Disabled
sd-wan	Red_Local (port9)	all	Noticias_php_443 Noticias_php_80	always	HTTP ALL_ICMP HTTPS	IPS SSL	ACCEPT	Enabled
sd-wan	Red_Local (port9)	all	MIP--189.204.131.154--172.20.22.18 corporativo.canal22 contenidos22.canal22.org.mx	always	HTTP HTTPS	IPS SSL	ACCEPT	Enabled
sd-wan	Red_Local (port9)	all	contenidos22.canal22.org.mx	always	HTTP HTTPS	IPS SSL	ACCEPT	Enabled
sd-wan	Red_Local (port9)	all	Publicacion_Canal22-80 Publicacion_Canal22-443	always	HTTP ALL_ICMP HTTPS TRACERROUTE	IPS SSL	ACCEPT	Enabled
sd-wan	Red_Local (port9)	all	Subdominios canal22	always	HTTP HTTPS PING	IPS SSL	ACCEPT	Enabled
sd-wan	Red_Local (port9)	all	Portal_Clic_Clac	always	HTTP ALL_ICMP HTTPS	IPS SSL	ACCEPT	Enabled
sd-wan	Red_Local (port9)	all	iluvatar iluvatar.443	always	HTTP ALL_ICMP HTTPS	IPS SSL	ACCEPT	Enabled
sd-wan	Red_Local (port9)	all	Publicacion_minisitios1	always	HTTP ALL_ICMP HTTPS	IPS SSL	ACCEPT	Enabled
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	resumen esya grass.valley promexar1 promexar2	10.100.10.0/24	always	ALL		ACCEPT	Disabled
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		ACCEPT	Disabled
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		ACCEPT	Disabled
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 jantonio.ruiz	10.100.10.0/24	always	ALL		ACCEPT	Disabled
SSL-VPN tunnel interface (ssl.root)	TVmetro_Invitados (invitados)	SSLVPN_TUNNEL_ADDR1 emilio_rene	172.31.226.0/24	always	ALL		ACCEPT	Disabled
SSL-VPN tunnel interface (ssl.root)	Canal 22 (canal22)	SSLVPN_TUNNEL_ADDR1 emilio_rene	172.31.227.0/24	always	ALL	+	ACCEPT	Disabled
SSL-VPN tunnel interface (ssl.root)	Eventos_Canal22 (canal22_eventos)	SSLVPN_TUNNEL_ADDR1 emilio_rene	172.31.228.0/24	always	ALL		ACCEPT	Disabled
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	IPS SSL	ACCEPT	Disabled
sd-wan	Red_Local (port9)	all	Desarrollo_443 Desarrollo Desarrollo_8080	always	8080/TCP HTTP HTTPS	IPS SSL	ACCEPT	Enabled
sd-wan	Red_Local (port9)	all	Publicacion_Programa	always	HTTP ALL_ICMP HTTPS	IPS SSL	ACCEPT	Enabled
sd-wan	Red_Local (port9)	all	Fireball	always	HTTP ALL_ICMP HTTPS	IPS SSL	ACCEPT	Enabled
Canal 22 (canal22)	sd-wan	172.31.227.0/24	www.centroculturaldigital.mx	always	ALL	WEB SSL APP	ACCEPT	Enabled
Eventos_Canal22 (canal22_eventos)	sd-wan	172.31.228.0/24	all	always	ALL	WEB SSL APP	ACCEPT	Enabled

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	+	ACCEPT Disabled
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		ACCEPT Disabled
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		ACCEPT Disabled
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		ACCEPT Disabled
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		ACCEPT Disabled
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		ACCEPT Disabled
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 10.252.10.0/26 172.16.1.0/24 172.31.200.0/23 172.31.215.0/24 172.31.221.0/24	always	ALL		ACCEPT Enabled

4. Top 10 de Firmas activadas por IPS por mes

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):

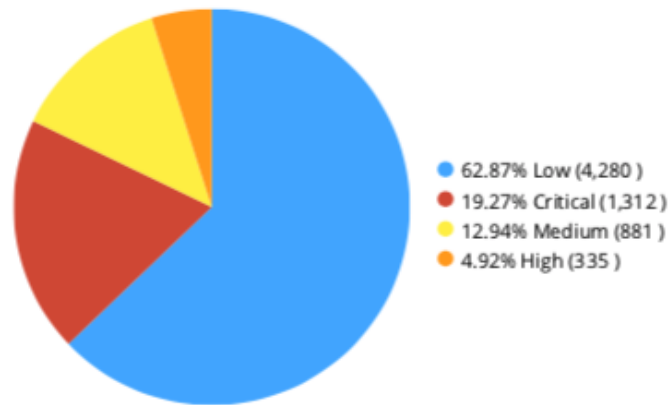
Edit Filter			
<input checked="" type="checkbox"/> Target: server <input checked="" type="checkbox"/> OS: Other <input checked="" type="checkbox"/> OS: Windows <input checked="" type="checkbox"/> OS: Linux <input checked="" type="checkbox"/> OS: Solaris <input checked="" type="checkbox"/> Application: Other <input checked="" type="checkbox"/> Application: IIS			
<input checked="" type="checkbox"/> Application: Apache <input checked="" type="checkbox"/> Application: Oracle <input checked="" type="checkbox"/> Application: MSSQL <input checked="" type="checkbox"/> Application: MySQL <input checked="" type="checkbox"/> Application: IE			
<input checked="" type="checkbox"/> Application: Mozilla <input checked="" type="checkbox"/> Application: MS_Office <input checked="" type="checkbox"/> Application: Adobe <input checked="" type="checkbox"/> Application: PHP_app <input checked="" type="checkbox"/> Application: ASP_app			
<input checked="" type="checkbox"/> Application: IM <input checked="" type="checkbox"/> Protocol: HTTP <input type="button" value="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.PerlIIS.dll.Remote.Buffer.Overflow		Server	Windows

< << 1 /61 >> [Total: 3010]

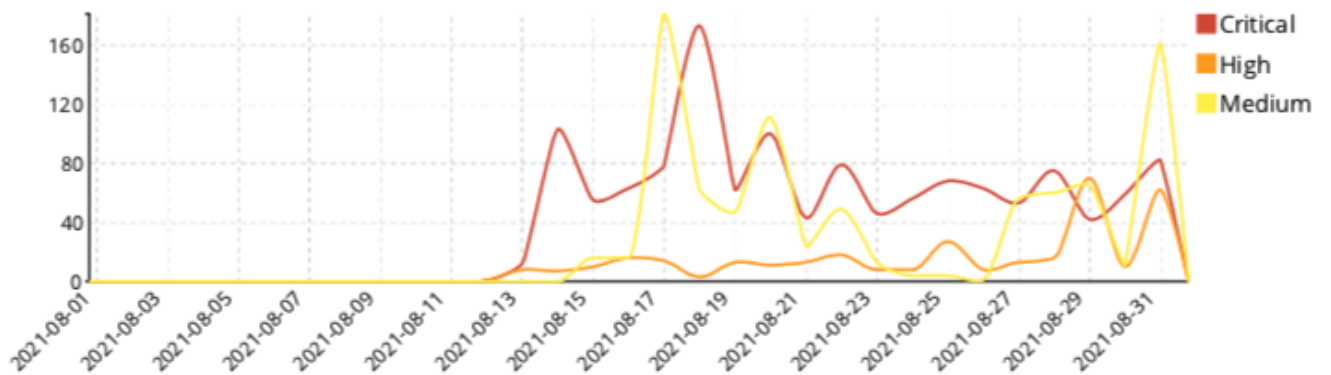
5. Top 10 de IPS con mayor consumo de Internet por mes

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

Intrusions By Severity














Critical High and Medium Intrusions Timeline



6. Detalle de los ataques detectados y detenidos

High Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	 HTTP.URL.SQL.Injection		SQL Injection	161
2	 Mirai.Botnet			132
3	 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-2021-2400,CVE-2018-13415,CVE-2018-13416,CVE-2018-13417,CVE-2018-15444,CVE-2018-18471,CVE-2019-17554,CVE-2019-18227,CVE-2019-18227,CVE-2020-15418,CVE-2020-15419,CVE-2020-26981,CVE-2021-21658,CVE-2021-21659,CVE-2021-21672,CVE-2021-29447	Other	16
4	 Multiple.Routers.syscmd.Remote.Command.Execution		OS Command Injection	13
5	 Generic.XXE.Detection	CVE-2012-3363,CVE-2013-4295,CVE-2013-5015,CVE-2014-3490,CVE-2016-9563,CVE-2018-8527,CVE-2018-8532,CVE-2018-8533,CVE-2019-0537,CVE-2019-0948,CVE-2019-2647,CVE-2019-2648,CVE-2019-2649,CVE-2019-2650,CVE-2020-0765,CVE-2018-13415,CVE-2018-13416,CVE-2018-13417,CVE-2018-15444,CVE-2018-18471,CVE-2019-17554,CVE-2019-18227,CVE-2019-18227,CVE-2020-15418,CVE-2020-15419,CVE-2020-26981,CVE-2021-21658,CVE-2021-21659,CVE-2021-21672,CVE-2021-29447	Other	3
6	 VACRON.CCTV.Board.CGI.cmd.Parameter.Command.Execution		OS Command Injection	3
7	 Tenda.AC15.AC1900.Authenticated.Remote.Command.Injection	CVE-2020-10987,CVE-2020-15916	OS Command Injection	2
8	 WordPress.Platform.Theme.Arbitrary.File.Upload		Permission/Privilege/Access Control	2
9	 JAWS.DVR.CCTV.Shell.Unauthenticated.Command.Execution		OS Command Injection	1
10	 Linksys.Routers.Administrative.Console.Authentication.Bypass		Permission/Privilege/Access Control	1
11	 WordPress.Web.API.Endpoint.Privilege.Escalation		Permission/Privilege/Access Control	1

Critical Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	CVE-2017-9841	Code Injection	591
2	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	CVE-2015-2051,CVE-2019-10891	OS Command Injection	156
3	WordPress.HTTP.Path.Traversal	CVE-2019-9618,CVE-2018-16283,CVE-2018-16299,CVE-2020-11738	Path Traversal	137
4	Dasan.GPON.Remote.Code.Execution	CVE-2018-10561,CVE-2018-10562	OS Command Injection	123
5	ThinkPHP.Controller.Parameter.Remote.Code.Execution	CVE-2019-9082,CVE-2018-20062	Code Injection	117
6	ZeroShell.Kerbynet.Type.Parameter.Remote.Command.Execution	CVE-2009-0545,CVE-2019-12725	Code Injection	93
7	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	CVE-2017-11317,CVE-2017-11357,CVE-2019-18935	Improper Authentication	29
8	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	CVE-2017-5638	Code Injection	24
9	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution		Code Injection	17
10	HTTP.URI.Java.Code.Injection	CVE-2018-1273	Code Injection	7
11	Red.Hat.JBoss.AS.doFilter.Insecure.Deserialization	CVE-2017-12149	OS Command Injection	4
12	Linux.Kernel.TCP.SACK.Panic.DoS	CVE-2019-11477,CVE-2019-11478,CVE-2019-11479	DoS	3
13	Gh0st.Rat.Botnet			3
14	Bladabindi.Botnet			3
15	D-Link.DSL-2750B.CLI.OS.Command.Injection		OS Command Injection	2
16	WordPress.Plugin.Userpro.Authentication.Bypass	CVE-2017-16562	Improper Authentication	1
17	MobileIron.MDM.Unauthenticated.Remote.Code.Execution	CVE-2020-15505	Permission/Privilege/Access Control	1
18	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	1

Medium Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	WordPress.xmlrpc.php.system.multicall.Amplification.Attack		Anomaly	636
2	Web.Server.Password.Files.Access		Permission/Privilege/Access Control	110
3	TCP.Split.Handshake		Anomaly	73
4	PHP.Diescan		Anomaly	48
5	WordPress.REST.API.Username Enumeration.Information.Disclosure	CVE-2017-5487	Information Disclosure	11
6	Mac.OSX.DSStore.Access.Content.Disclosure		Information Disclosure	2
7	WordPress.Plugin.Social.Warfare.XSS	CVE-2019-9978	XSS	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	591
2	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	Critical	156
3	WordPress.HTTP.Path.Traversal	Critical	137
4	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Critical	117
5	Dasan.GPON.Remote.Code.Execution	Critical	111
6	Zeroshell.Kerbynet.Type.Parameter.Remote.Command.Execution	Critical	93
7	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Critical	28
8	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Critical	23
9	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Critical	12
10	Bladabindi.Botnet	Critical	3
11	Linux.Kernel.TCP.SACK.Panic.DoS	Critical	3
12	Gh0st.Rat.Botnet	Critical	3
13	Red.Hat.JBoss.AS.doFilter.Insecure.Deserialization	Critical	3
14	D-Link.DSL-2750B.CLI.OS.Command.Injection	Critical	2
15	WordPress.Plugin.Userpro.Authentication.Bypass	Critical	1
16	Bash.Function.Definitions.Remote.Code.Execution	Critical	1
17	MobileIron.MDM.Unauthenticated.Remote.Code.Execution	Critical	1
18	HTTP.URI.SQL.Injection	High	161
19	Mirai.Botnet	High	132
20	Generic.XXE.Detection	High	19
21	Multiple.Routers.syscmd.Remote.Command.Execution	High	12
22	WordPress.Platform.Theme.Arbitrarily.File.Upload	High	2
23	WordPress.Web.API.Endpoint.Privilege.Escalation	High	1
24	WordPress.xmlrpc.php.system.mutualAmplification.Attack	Medium	636
25	Web.Server.Password.Files.Access	Medium	110

7. Reporte de FireWall de Aplicaciones

7.1. Incidentes detectados y contenidos por mes

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

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

Evidencias

Intrusion Victims

#	Attack Victim	Counts	Percent of Total Attacks
1	10.0.0.218		515 20.37%
2	172.20.22.44		410 16.22%
3	10.0.0.211		292 11.55%
4	172.20.22.11		219 8.66%
5	172.20.22.35		156 6.17%
6	172.20.22.18		120 4.75%
7	172.20.22.25		115 4.55%
8	10.0.0.208		112 4.43%
9	10.252.10.20		108 4.27%
10	172.20.22.12		104 4.11%
11	10.0.0.216		100 3.96%
12	10.0.0.209		95 3.76%
13	10.0.0.202		94 3.72%
14	10.0.0.207		85 3.36%
15	134.122.112.12		2 0.08%
16	10.0.0.219		1 0.04%

Intrusion Sources

#	Attack Source	Counts	Percent of Total Attacks
1	45.146.164.110		640 57.71%
2	46.4.55.140		110 9.92%
3	154.16.180.213		50 4.51%
4	162.210.70.9		46 4.15%
5	103.53.42.51		43 3.88%
6	203.248.175.72		25 2.25%
7	95.128.43.164		23 2.07%
8	51.161.61.87		22 1.98%
9	154.16.180.212		19 1.71%
10	61.155.0.253		15 1.35%
11	20.102.74.72		13 1.17%
12	18.177.137.39		12 1.08%
13	193.242.145.12		12 1.08%
14	194.182.182.193		12 1.08%
15	180.242.192.84		12 1.08%
16	20.42.104.6		12 1.08%
17	87.106.204.238		11 0.99%
18	20.106.72.153		11 0.99%
19	203.248.175.71		11 0.99%
20	140.206.86.125		10 0.90%

8. Tipo y número de ataques detectados y detenidos

8.1. Top 10 de URLs utilizadas por mes

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

URL	Type	Action	Status
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.typekit.net	Wildcard	Allow	Enable
www.google-analytics.com	Wildcard	Allow	Enable
www.youtube.com	Wildcard	Allow	Enable
fonts.gstatic.com	Wildcard	Allow	Enable
iytimg.com	Wildcard	Allow	Enable
yt3.ggpht.com	Wildcard	Allow	Enable
static.doubleclick.net	Wildcard	Allow	Enable
centroculturaldigital	Wildcard	Allow	Enable
http://www.centroculturaldigital.mx	Wildcard	Allow	Enable
*centroculturaldigital.mx	Wildcard	Allow	Enable
https://www.mitelcel.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

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.centroculturaldigital.mx*	Western	Exempt	Enable
Wildcard	gnula.nu	Western	Exempt	Enable
Wildcard	*gemajoyeria.com*	Western	Exempt	Enable
Wildcard	*tucargasegura.com*	Western	Exempt	Enable

Intrusions Blocked

#	Intrusion Name	Intrusion Type	Severity	Counts
1	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Code Injection	Critical	591
2	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	Critical	156
3	WordPress.HTTP.Path.Traversal	Path Traversal	Critical	137
4	Dasan.GPON.Remote.Code.Execution	OS Command Injection	Critical	123
5	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Code Injection	Critical	117
6	Zeroshell.Kerbynet.Type.Parameter.Remote.Command.Execution	Code Injection	Critical	93
7	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Improper Authentication	Critical	29
8	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Code Injection	Critical	24
9	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection	Critical	17
10	HTTP.URI.Java.Code.Injection	Code Injection	Critical	7
11	Red.Hat.jBoss.AS.doFilter.Insecure.Deserialization	OS Command Injection	Critical	4
12	Gh0st.Rat.Botnet		Critical	3
13	Linux.Kernel.TCP_SACK.Panic.DoS	DoS	Critical	3
14	Bladabindi.Botnet		Critical	3
15	D-Link.DSL-2750B.CLI.OS.Command.Injection	OS Command Injection	Critical	2
16	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	Critical	1
17	WordPress.Plugin.Userpro.Authentication.Bypass	Improper Authentication	Critical	1
18	MobileIron.MDM.Unauthenticated.Remote.Code.Execution	Permission/Privilege/Access Control	Critical	1
19	HTTP.URI.SQL.Injection	SQL Injection	High	161
20	Mirai.Botnet		High	132

9. 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	28,987

10. Top 10 de IPS con mayor consumo de ancho de banda

Top 20 Bandwidth Users

#	User (or IP)	Bandwidth
1	 10.100.1.27	100.21 GB
2	 172.16.1.185	60.75 GB
3	 172.16.1.108	17.51 GB
4	 172.16.1.1	15.13 GB
5	 172.31.226.101	14.07 GB
6	 172.31.215.168	13.76 GB
7	 172.16.1.153	12.31 GB
8	 10.100.1.61	12.09 GB
9	 172.16.1.137	11.54 GB
10	 172.31.226.11	9.75 GB
11	 172.16.1.208	9.07 GB
12	 172.31.226.13	8.89 GB
13	 172.16.1.4	8.79 GB
14	 172.16.1.85	8.54 GB
15	 172.16.1.245	8.26 GB
16	 172.16.1.6	7.72 GB
17	 172.16.1.55	6.86 GB
18	 172.16.1.21	6.58 GB
19	 172.16.1.200	6.41 GB
20	 172.16.1.107	6.39 GB

11. Reporte de Acceso y Publicación a 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	172.31.201.168		718.10 GB		27,342
2	172.31.200.139		712.62 GB		747,022
3	172.31.201.127		469.00 GB		66,708
4	172.31.200.153		441.32 GB		2,620,933
5	172.31.201.64		347.67 GB		1,103,415
6	172.31.200.72		342.14 GB		28,908
7	172.31.201.205		337.82 GB		316,379
8	172.31.201.235		313.47 GB		691,574
9	172.31.200.38		263.12 GB		5,996
10	172.31.200.101		250.82 GB		17,679
11	172.31.200.90		196.81 GB		102,982
12	172.31.201.17		184.07 GB		27,901
13	10.100.4.1		144.66 GB		1,198
14	10.252.10.8		115.12 GB		298
15	172.20.22.19		113.94 GB		68,055,451
16	172.31.201.25		110.16 GB		17,951
17	10.100.1.27		108.03 GB		1,821,408
18	10.100.4.2		101.86 GB		590
19	10.100.4.3		99.46 GB		1,675
20	172.31.215.168		90.83 GB		147,204
21	10.252.10.7		75.15 GB		1,813
22	172.31.200.250		73.55 GB		190,305
23	172.31.201.199		68.39 GB		375,237
24	172.31.200.79		68.38 GB		11,510
25	172.31.200.30		67.73 GB		110,359
26	172.31.200.247		66.35 GB		30,946
27	172.31.200.104		64.54 GB		54,448
28	172.16.1.185		63.90 GB		226,783
29	172.31.200.70		58.54 GB		31,924
30	172.31.201.204		56.39 GB		335,175

12. 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.

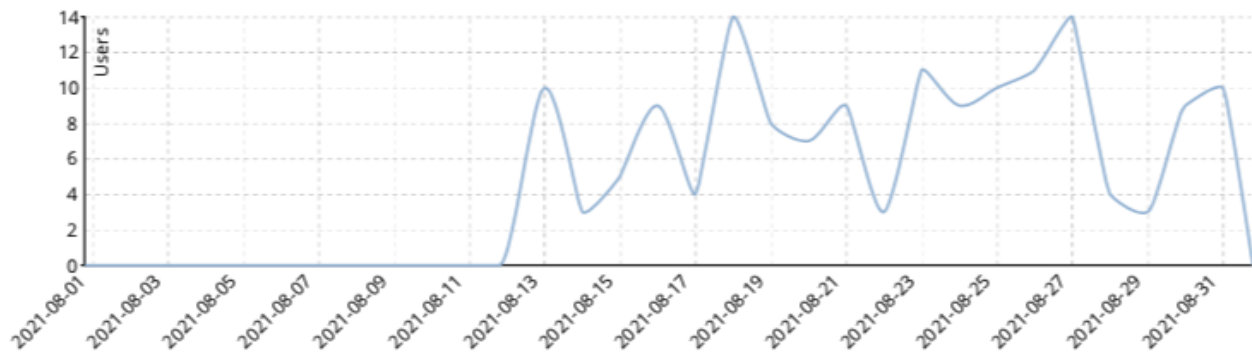
A continuación, se muestran los consumos por categoría de aplicaciones:

Application Categories by Bandwidth











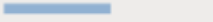





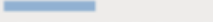


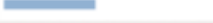


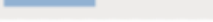



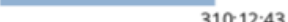

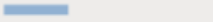

#	Application Category	Bandwidth
1	Video/Audio	690.62 GB
2	Web.Client	651.74 GB
3	Collaboration	284.76 GB
4	Social.Media	202.31 GB
5	Email	166.83 GB
6	Network.Service	52.56 GB
7	General.Interest	46.37 GB
8	Update	40.08 GB
9	Unknown	36.79 GB
10	Remote.Access	29.92 GB

13. Consumo de usuarios de VPN





















VPN User Logins



Authenticated Logins

#	User	Type	First Used	Total Number of Connections	Total Duration Connected(HH:MM:SS)
1	 alejandro.martinez	ssl-tunnel	2021-08-13 22:47:52	 39	 99:09:56
2	 pedro.rodriguez	ssl-tunnel	2021-08-13 08:00:34	 33	 122:02:03
3	 luis.noguez	ssl-tunnel	2021-08-13 15:40:13	 22	 111:17:51
4	 daniela	ssl-tunnel	2021-08-16 09:25:53	 20	 81:56:04
5	 abigail	ssl-tunnel	2021-08-13 11:59:25	 19	 05:20:00
6	 javier.rosario	ssl-tunnel	2021-08-13 09:32:28	 17	 09:28:38
7	 alexis.lopez	ssl-tunnel	2021-08-13 12:39:57	 17	 22:51:19
8	 jantonio.ruiz	ssl-tunnel	2021-08-19 12:51:54	 17	 35:39:03
9	 C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FG3K9B3E12700361, emailAddress = support@fortinet.com	ipsec	2021-08-19 01:39:08	 14	 310:12:43
10	 claudia	ssl-tunnel	2021-08-13 23:06:54	 12	 29:27:55

Failed Login Attempts

#	User	Type	Total Number of Failed Attempts
1	 administrator	ssl-web	 638
2	 administrador	ssl-web	 52
3	 admin	ssl-web	 8
4	 javier.rosario	ssl-web	 5
5	 User	ssl-web	 4
6	 vpn	ssl-web	 4
7	 vpnuser	ssl-web	 4
8	 eadmin	ssl-web	 3
9	 jadmin	ssl-web	 2
10	 zadmin	ssl-web	 2



Reporte de Acceso y Publicación a Internet

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

AGOSTO 2021

Información General del Documento

Entregable	Clave	Servicio	Medio
	E02 - API	Reporte de Acceso y Publicación a Internet	Electrónico

Elaboración	Puesto	Nombre
	Responsable del Servicio	Edgar Abraham Leones Rodríguez

Revisión	Puesto	Nombre
	Líder de proyecto	Victor Quiroz Barrientos

Aprobación	Puesto	Nombre
	Encargado de la Gerencia de Administración Integral e Infraestructura	Rubén Darío Sarmiento Gómez

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

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

Tabla de contenido

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

1. Introducción

El presente documento muestra un resumen de las actividades realizadas como parte del Servicio de Telecomunicaciones que actualmente el **CANAL 22** tiene contratados con el 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

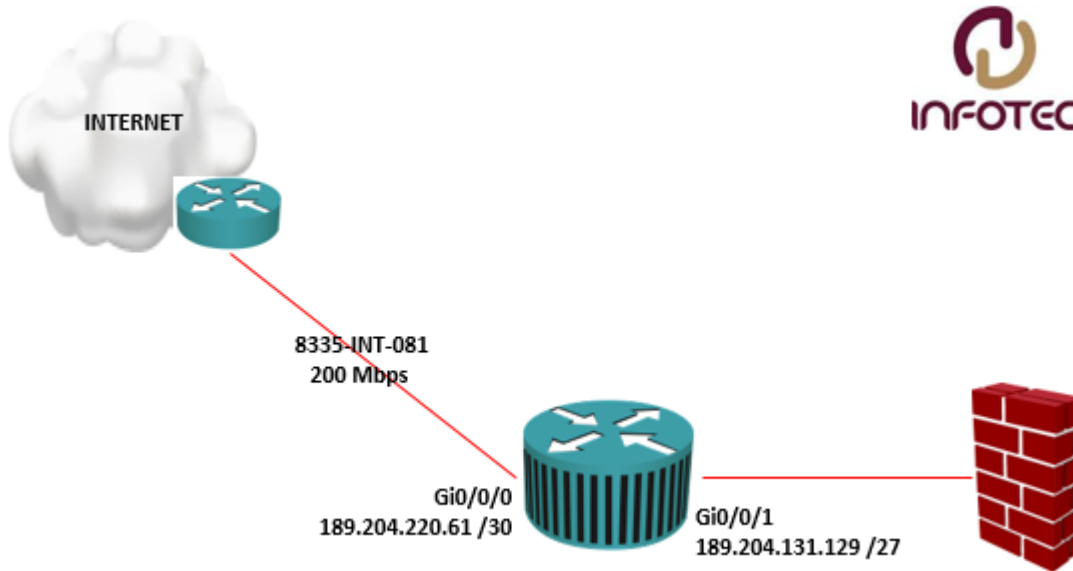
El presente documento tiene como objetivo reportar la disponibilidad de los enlaces contratados por el **CANAL 22**, el cual está integrado por un diagrama de topología de red y graficas que muestran la utilización de tráfico servicios de Acceso y Publicación a Internet, así como el intercambio de tráfico.

La comprobación de la prestación de los servicios que se informan en este documento corresponde a la operación del **01 de agosto al 31 de agosto 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.



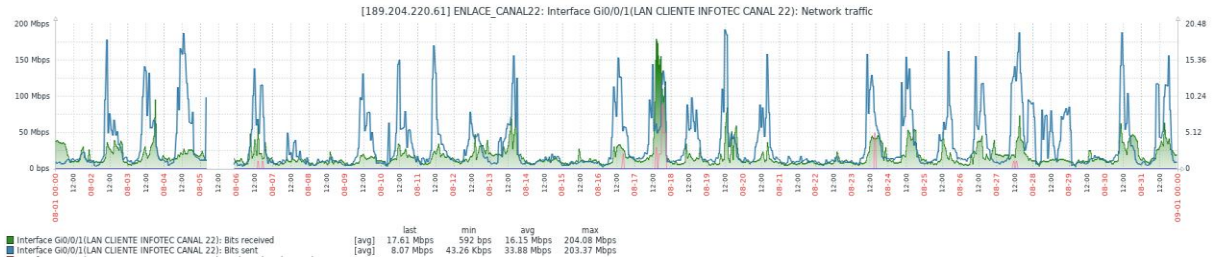
Red de Publicación a INTERNET		
VLAN	DIRECCIONAMIENTO IP	DESCRIPCIÓN
Por definir	189.204.131.128/27	Administración y Monitoreo

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.

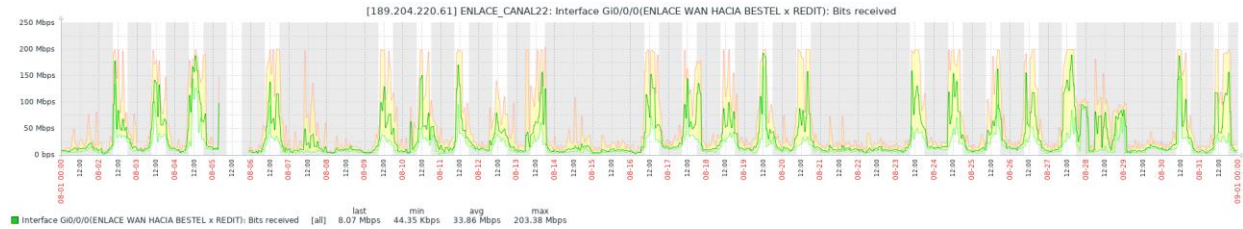
Durante el mes de agosto se presentaron los siguientes datos en la interfaz donde llega el enlace:

- Entradas de tráfico de un **promedio de 16.15 Mbps.**
- Salidas de tráfico de un **promedio de 33.88 Mbps.**



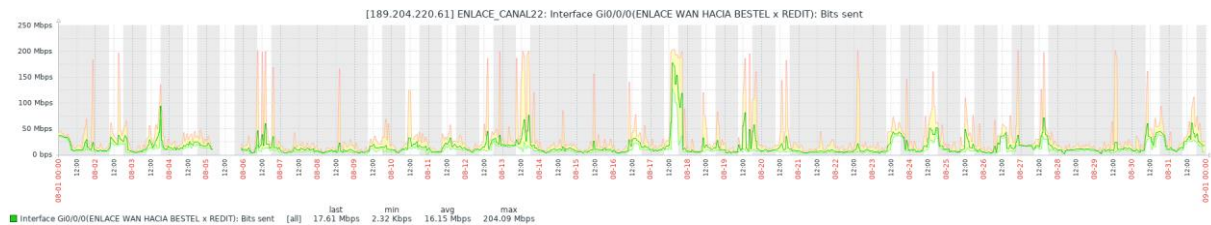
Trafico entrada

El *pico máximo de entrada* de acceso y publicación a internet correspondiente es de **203.38 Mbps.**

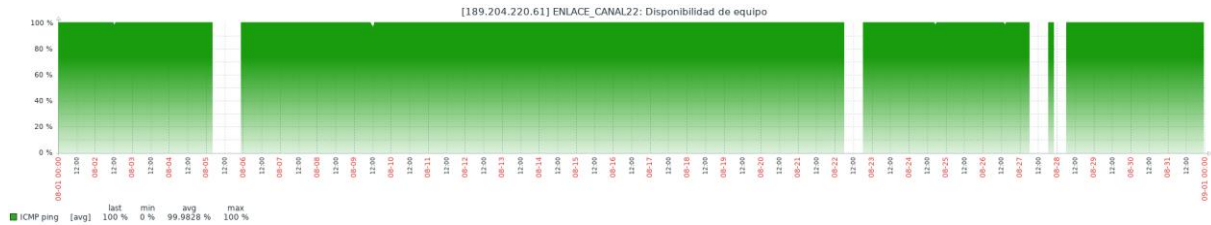


Trafico salida

El *pico máximo de salida* de acceso y publicación a internet correspondiente es de **204.09 Mbps.**



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



5. Glosario de Términos

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

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

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

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

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

Volume

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

Availability

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

Utilization

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

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

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

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

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

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

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

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

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

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

Discard Rate

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

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

Exceptions

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

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

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

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

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

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

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

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



Reporte de Incidentes y Solicitudes de Mesa de Servicios

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

AGOSTO 2021



Firmas de revisión, aprobación y recepción del documento.

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

Elaboración	Puesto	Nombre	Fecha
	Supervisor de Mesa de Servicios	Gerardo Diego Huerta Clemente	3/09/2021

Revisión	Puesto	Nombre	Fecha
	Coordinador de Mesa de Servicios	Alejandro Rubén de la Cruz Ornelas	03/09/2021

Aprobación	Puesto	Nombre	Fecha
	Líder de Proyecto	Victor Quiroz Barrientos	03/09/2021

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

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 AGOSTO 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.

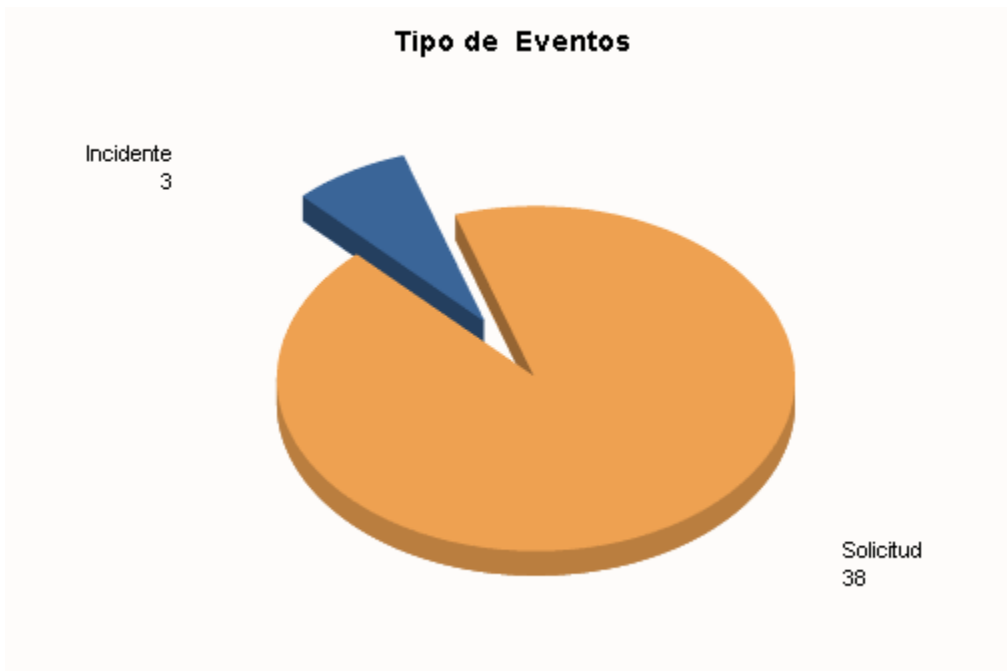
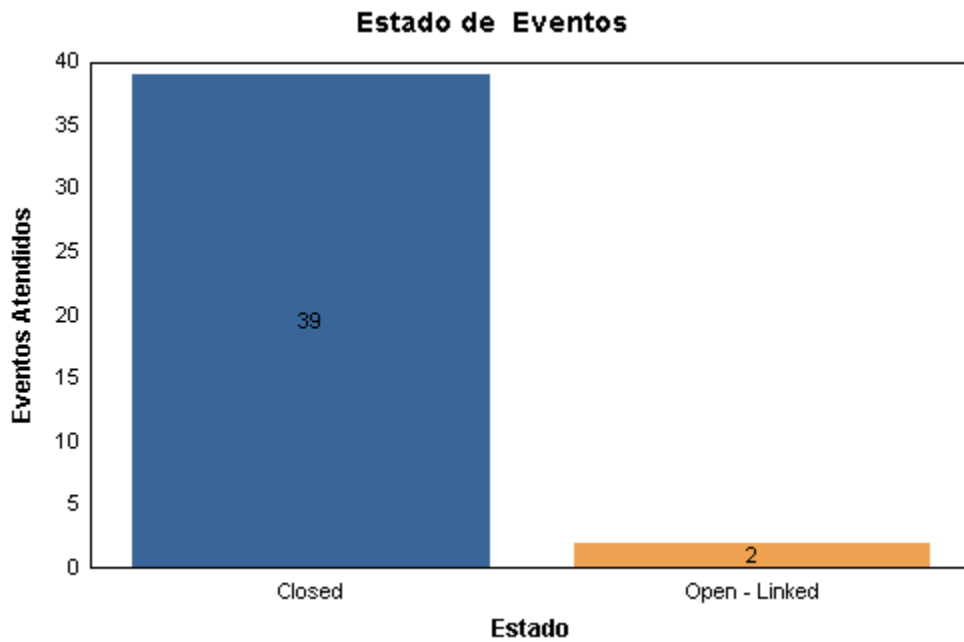
Al final, encontrará un glosario donde se definen los términos utilizados en este documento.

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.

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: ALERTA CANAL 22 / <https://portalproyectos.canal22.org.mx/> / URL NO RESPONDE
Descripción: CLIENTE: CANAL22
URL: <https://portalproyectos.canal22.org.mx/>
ALERTA: URL NO RESPONDE

Atendido por: GUEVARA MORALES, TERESA_
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 21/08/2021 03:52:03a.m.
Ticket asignado: TK317800
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Incidente

Solución: 21/08/2021 09:56 Hrs. En atencion al evento se reciben comentarios de la Ing. Andrea Karina de
Monitoreo:

La pagina responde se anexa evidencia

Fecha y hora de cierre: 21/08/2021 11:49:32a.m.
Tiempo total del Ticket: 00 07:57:29

Título: ALERTA CANAL 22/ [https://noticias.canal22.org.mx/?/](https://noticias.canal22.org.mx?/) / URL no responde
Descripción: Por medio del presente se reporta la siguiente alerta de monitoreo

CLIENTE: CANAL 22

URL: <https://noticias.canal22.org.mx>
ALERTA: URL no responde
Quedo atenta a sus comentarios | Saludos Cordiales

Atendido por: HUERTA CLEMENTE, GERARDO DIEGO.
Usuario que abre evento: QUIROZ BARRIENTOS, _VICTOR
Fecha y hora de apertura: 24/08/2021 09:56:01a.m.
Ticket asignado: TK317905
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Incidente



CANAL 22

Detalle de Eventos

Solución: 24/08/2021 09:58 Hrs. en atención al evento nos comunicamos con el ing. Emilio Rene de CANAL22 para reportarle la falla y le comentamos sobre que el tema es del servidor y nos dice que ya se soluciono que estabilizo el servidor y que probamos de nuevo la URL, misma que ya esta respondiendo correctamente, saludos

Fecha y hora de cierre: 24/08/2021 07:04:09p.m.
Tiempo total del Ticket: 00 09:08:08

Título: Falla internet_CANAL 22
Descripción: Estamos reportando fallas en el internet por favor revisen si hay algún problema.

Quedo al pendiente de su respuesta

Atendido por: CARLOS CRUZ, ELIDETH
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 20/08/2021 07:13:09p.m.
Ticket asignado: TK317790
Medio de contacto: Correo electronico
Estado evento: Abierto con Registro Relacionado
Clasificación: Incidente

Título: Reporte de consumo de ancho de banda-2021-08-01-1000_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.

Se adjunta el reporte.

Atendido por: RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 01/08/2021 10:03:31a.m.
Ticket asignado: TK316887
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud



CANAL 22

Detalle de Eventos

Solución: 01/08/21 10:03 Hrs En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 01/08/2021 10:42:53p.m.

Tiempo total del Ticket: 00 12:39:22

Título: Reporte de consumo de ancho de banda-2021-08-02-1000 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: 02/08/2021 10:02:46a.m.

Ticket asignado: TK316901

Medio de contacto: Correo electronico

Estado evento: Cerrado

Clasificación: Solicitud

Solución: 02/08/2021 10:05 Hrs En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 02/08/2021 09:42:38p.m.

Tiempo total del Ticket: 00 11:39:52



CANAL 22

Detalle de Eventos

Título: Certificado SSL noticias.canal22.org.mx_CANAL 22
Descripción: Solicito su ayuda para sustituir en el certificado SSL adjunto para el sitio noticias.canal22.org.mx

Quedo al pendiente de sus comentarios.

Atendido por: CARLOS CRUZ, ELIDETH
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 02/08/2021 11:05:24a.m.
Ticket asignado: TK316907
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 04/08/2021 21:07 Hrs. En atención al evento se reciben comentarios por parte del Ing. Kevin Vazquez del SOC:
Se ha realizado el cambio de certificado y validado el funcionamiento.

Fecha y hora de cierre: 04/08/2021 11:07:12p.m.
Tiempo total del Ticket: 02 12:01:48

Título: Reporte de consumo de ancho de banda-2021-08-03-1000 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



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: 03/08/2021 10:05:56a.m.
Ticket asignado: TK316964
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 03/08/2021 10:05 Hrs En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 03/08/2021 09:45:28p.m.
Tiempo total del Ticket: 00 11:39:32

Título: Urgente Falla DNS comercial.canal22.org.mx
Descripción: Solicito su ayuda para revisar el DNS comercial.canal22.org.mx debido a que no esta resolviendo.

Adjunto el formato de DNS de como deberá estar configurado.

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 03/08/2021 12:12:11p.m.
Ticket asignado: TK316972
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 03/08/2021 12:49 Hrs. En atención al evento, se reciben comentarios por parte del Ing. Emilio Rene de CANAL 22

El servicio esta reestablecido muchas gracias, pueden cerrar el TK.

Fecha y hora de cierre: 03/08/2021 01:44:48p.m.
Tiempo total del Ticket: 00 01:32:37



CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-08-04-1000_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: CARLOS CRUZ, ELIDETH
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 04/08/2021 10:05:10a.m.
Ticket asignado: TK317019
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 04/08/2021 10:07 Hrs En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 04/08/2021 11:07:04p.m.
Tiempo total del Ticket: 00 13:01:54

Título: Reporte de consumo de ancho de banda-2021-08-05-1000-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: CARLOS CRUZ, ELIDETH
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 05/08/2021 10:06:25a.m.
Ticket asignado: TK317083
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud



CANAL 22

Detalle de Eventos

Solución: 05/08/2021 10:07 Hrs En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 05/08/2021 09:50:10p.m.
Tiempo total del Ticket: 00 11:43:45

Título: Reporte de consumo de ancho de banda-2021-08-06-1000 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: 06/08/2021 10:07:38a.m.
Ticket asignado: TK317127
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 06/08/2021 10:12 Hrs En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 08/08/2021 10:06:42p.m.
Tiempo total del Ticket: 02 11:59:04



CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-08-07-1000_CANAL 22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 07/08/2021 10:06:15a.m.
Ticket asignado: TK317182
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 07/08/2021 10:00 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 08/08/2021 10:08:06p.m.
Tiempo total del Ticket: 01 12:01:51

Título: Reporte de consumo de ancho de banda-2021-08-08-1000_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: 08/08/2021 10:03:17a.m.
Ticket asignado: TK317191
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 08/08/2021 10:07 Hrs. Ingenieros, les informamos que se registró el TK317191 solicitando de su apreciable apoyo para brindar atención al evento que se describe en el correo que antecede.



CANAL 22

Detalle de Eventos

Fecha y hora de cierre: 08/08/2021 10:09:45p.m.
Tiempo total del Ticket: 00 12:06:28

Título: Reporte de consumo de ancho de banda-2021-08-09-1000_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.

Atendido por: GONZALEZ CURENO, ROGELIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 09/08/2021 10:03:59a.m.
Ticket asignado: TK317202
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 09/08/2021 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: 09/08/2021 09:59:31p.m.
Tiempo total del Ticket: 00 11:55:32

Título: Reporte de consumo de ancho de banda-2021-08-10-1000 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



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: 10/08/2021 10:04:53a.m.
Ticket asignado: TK317264
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 10/08/2021 10:07 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 10/08/2021 10:24:37p.m.
Tiempo total del Ticket: 00 12:19:44

Título: Reporte de consumo de ancho de banda-2021-08-11-1000_CANAL 22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: GONZALEZ CURENO, ROGELIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 11/08/2021 10:03:44a.m.
Ticket asignado: TK317310
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 11/08/2021 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: 12/08/2021 01:49:22a.m.
Tiempo total del Ticket: 00 15:45:38



CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-08-12-1000_CANAL22
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: CARLOS CRUZ, ELIDETH
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 12/08/2021 10:04:37a.m.
Ticket asignado: TK317365
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 12/08/2021 10:06 Hrs En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 12/08/2021 10:12:11p.m.
Tiempo total del Ticket: 00 12:07:34

Título: Reporte de consumo de ancho de banda-2021-08-13-1000_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: GONZALEZ CURENO, ROGELIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 13/08/2021 10:06:45a.m.
Ticket asignado: TK317422
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud



CANAL 22

Detalle de Eventos

Solución: 13/08/2021 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: 15/08/2021 08:20:54p.m.
Tiempo total del Ticket: 02 10:14:09

Título: Reporte de consumo de ancho de banda-2021-08-14-1000_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.

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 14/08/2021 10:07:41a.m.
Ticket asignado: TK317474
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 14/08/2021 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: 15/08/2021 08:24:48p.m.
Tiempo total del Ticket: 01 10:17:07

Título: Reporte de consumo de ancho de banda-2021-08-15-1000
Descripción: Buenos días,

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

Se adjunta el reporte.



CANAL 22

Detalle de Eventos

Atendido por: MORALES FAJARDO, LUIS ALBERTO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 15/08/2021 10:03:13a.m.
Ticket asignado: TK317485
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 15/08/2021 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: 15/08/2021 08:25:33p.m.
Tiempo total del Ticket: 00 10:22:20

Título: Reporte de consumo de ancho de banda-2021-08-16-1000_CANAL 22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: GONZALEZ CURENO, ROGELIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 16/08/2021 10:05:51a.m.
Ticket asignado: TK317498
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 16/08/2021 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: 17/08/2021 08:13:59p.m.
Tiempo total del Ticket: 01 10:08:08



CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-08-17-1000 CANAL22
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: HUERTA CLEMENTE, GERARDO DIEGO.
Usuario que abre evento: QUIROZ BARRIENTOS, _VICTOR
Fecha y hora de apertura: 17/08/2021 10:10:07a.m.
Ticket asignado: TK317558
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 17/08/2021 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: 17/08/2021 08:16:03p.m.
Tiempo total del Ticket: 00 10:05:56

Título: Reporte de consumo de ancho de banda-2021-08-18-1000_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: 18/08/2021 10:03:53a.m.
Ticket asignado: TK317624
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud



CANAL 22

Detalle de Eventos

Solución: 18/08/2021 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: 18/08/2021 11:06:46p.m.

Tiempo total del Ticket: 00 13:02:53

Título: Certificado SSL corporativo.canal22.org.mx

Descripción: Solicito su ayuda para renovar el certificado SSL al portal web <https://corporativo.canal22.org.mx> con el siguiente NAT.

Nombre Publicado Firewall

IP Publica

WAF

IP Interna

corporativo

189.204.131.142

10.0.0.218

172.20.22.35

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



CANAL 22

Detalle de Eventos

Atendido por: CARLOS CRUZ, ELIDETH
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 18/08/2021 11:56:29a.m.
Ticket asignado: TK317634
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 18/08/2021 23:12 hrs. En atención al evento se reciben comentarios del Ing. Kevin Vazquez de SOC:

Se ha cargado el certificado proporcionado

Fecha y hora de cierre: 19/08/2021 02:52:17a.m.
Tiempo total del Ticket: 00 14:55:48

Título: Reporte de consumo de ancho de banda-2021-08-19-1000 CANAL22
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: HUERTA CLEMENTE, GERARDO DIEGO.
Usuario que abre evento: QUIROZ BARRIENTOS, _VICTOR
Fecha y hora de apertura: 19/08/2021 10:03:23a.m.
Ticket asignado: TK317695
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 19/08/2021 10:05 Hrs. en atención al evento se recibe comentarios del especialista de SOC:
Se adjunta el reporte.

Fecha y hora de cierre: 20/08/2021 12:01:48p.m.
Tiempo total del Ticket: 01 01:58:25



CANAL 22

Detalle de Eventos

Título: Realizar Alta VLAN 103_ CANAL22
Descripción: Estimados

Buenas tardes

Solicito su ayuda para dar de alta la VLAN 103 con las siguientes características:

Descripcion: Streaming equipos Teradeck
VLAN ID 103
Network: 10.100.4.0/29
Netmask: 255.255.255.248 = 29
Broadcast: 10.100.4.6
Hosts/Net: 8

Quedo al pendiente de cualquier duda o aclaración

Saludos.

Atendido por: HUERTA CLEMENTE, GERARDO DIEGO.
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 19/08/2021 08:08:25p.m.
Ticket asignado: TK317741
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 20/08/2021 12:10 Hrs. En atención al evento se reciben comentarios del Ing. Kevin Vazquez :

Se ha realizado la configuración y validado en conjunto con el cliente

Fecha y hora de cierre: 20/08/2021 10:10:19p.m.
Tiempo total del Ticket: 01 02:01:54



CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-08-20-1000_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.

Atendido por: GONZALEZ CURENO, ROGELIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 20/08/2021 10:02:50a.m.
Ticket asignado: TK317765
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 20/08/2021 10:00 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 20/08/2021 12:00:52p.m.
Tiempo total del Ticket: 00 01:58:02

Título: Quitar politica de acceso a internet_CANAL 22
Descripción: Buena tarde

Solicito su ayuda para quitar la política que impide el acceso a internet al siguiente rango de IPs 10.100.10.34 a 10.100.10.43 con la finalidad de realizar actualizaciones en los equipos, una vez que se termine el proceso de actualización les informaremos para colocar nuevamente la política que impide el acceso a internet.

Quedo al pendiente de cualquier duda o actualización

Atendido por: GONZALEZ CURENO, ROGELIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 20/08/2021 02:21:15p.m.
Ticket asignado: TK317780
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud



CANAL 22

Detalle de Eventos

Solución: 20/08/2021 17:01 Hrs. En cancelación al evento se reciben comentarios del Ing. Emilio García de CANAL 22 :

Favor de cerrar el tíquet sin aplicar la configuración.

Fecha y hora de cierre: 24/08/2021 06:58:47p.m.
Tiempo total del Ticket: 04 04:37:32

Título: Reporte de consumo de ancho de banda-2021-08-21-1000_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.

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 21/08/2021 10:05:26a.m.
Ticket asignado: TK317815
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 21/08/2021 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: 24/08/2021 07:00:45p.m.
Tiempo total del Ticket: 03 08:55:19

Título: Reporte de consumo de ancho de banda-2021-08-22-1000_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.



CANAL 22

Detalle de Eventos

Atendido por: RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 22/08/2021 10:07:32a.m.
Ticket asignado: TK317830
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 22/08/2021 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: 24/08/2021 07:03:43p.m.
Tiempo total del Ticket: 02 08:56:11

Título: Reporte de consumo de ancho de banda-2021-08-23-1000_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: GONZALEZ CURENO, ROGELIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 23/08/2021 10:03:11a.m.
Ticket asignado: TK317851
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 23/08/2021 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: 24/08/2021 07:02:41p.m.
Tiempo total del Ticket: 01 08:59:30



CANAL 22

Detalle de Eventos

Título: URGENTE REVISAR CERTIFICADO DE PORTAL CORPORATIVO
Descripción: el portal web <https://corporativo.canal22.org.mx/> esta fallando ya que no esta instalado correctamente el certificado SSL se sugiere revisar la instalacion en el siguiente portal<https://www.whynopadlock.com/>

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 24/08/2021 07:06:55p.m.
Ticket asignado: TK317927
Medio de contacto: Telefono
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 26/08/2021 16:26 Hrs. En atencion al evento se reciben comentarios del Ing. Kevin Vazquez del SOC:

Se ha realizado la carga del certificado de manera correcta, favor de revisar del lado del cliente que la configuración sea correcta.

Fecha y hora de cierre: 26/08/2021 09:32:23p.m.
Tiempo total del Ticket: 02 02:25:28

Título: Reporte de consumo de ancho de banda-2021-08-25-1000_CANAL 22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: GONZALEZ CURENO, ROGELIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 25/08/2021 10:02:54a.m.
Ticket asignado: TK317954
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 25/08/2021 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: 26/08/2021 05:00:47a.m.
Tiempo total del Ticket: 00 18:57:53

Título: Reporte de consumo de ancho de banda-2021-08-26-1000 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: 26/08/2021 10:09:48a.m.
Ticket asignado: TK318001
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 26/08/2021 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: 26/08/2021 10:59:16p.m.
Tiempo total del Ticket: 00 12:49:28



CANAL 22

Detalle de Eventos

Título: Alta VLAN ID 104_CANAL 22
Descripción: Estimados

Buenas tardes

Solicito su ayuda para dar de alta la VLAN 104 con las siguientes características:

- Descripción: VLAN para realizar servicios de prueba
- VLAN ID 104
- Network: 10.100.5.0/29
- Netmask: 255.255.255.248 = 29
- Broadcast: 10.100.5.6
- Hosts/Net: 8

Por ultimo agregar a esta VLAN 104 las mismas politicas de navegacion que tiene la VLAN 103.

Quedo al pendiente de cualquier duda o aclaración

Atendido por: HUERTA CLEMENTE, GERARDO DIEGO.
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 26/08/2021 02:37:56p.m.
Ticket asignado: TK318019
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 26/08/2021 22:57 Hrs. En atención al evento se reciben comentarios del Ing. Kevin Vázquez de SOC.
Se ha realizado el alta de la VLAN 104 y configurado las mismas políticas de la Vlan 103

Fecha y hora de cierre: 27/08/2021 04:11:41a.m.
Tiempo total del Ticket: 00 13:33:45



CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-08-27-1000_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: CARLOS CRUZ, ELIDETH
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 27/08/2021 10:05:18a.m.
Ticket asignado: TK318053
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 27/08/2021 10:06 Hrs En atencion al evento se reciben comentarios por parte de SOC:
Se adjunta el reporte.

Fecha y hora de cierre: 27/08/2021 09:35:55p.m.
Tiempo total del Ticket: 00 11:30:37

Título: Reporte de consumo de ancho de banda-2021-08-28-1000_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: 28/08/2021 10:01:49a.m.
Ticket asignado: TK318098
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud



CANAL 22

Detalle de Eventos

Solución: 28/08/2021 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: 29/08/2021 12:15:10p.m.
Tiempo total del Ticket: 01 02:13:21

Título: Reporte de consumo de ancho de banda-2021-08-29-1000_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: 29/08/2021 10:03:48a.m.
Ticket asignado: TK318110
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 29/08/2021 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: 29/08/2021 01:14:04p.m.
Tiempo total del Ticket: 00 03:10:16



CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-08-30-1000 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: 30/08/2021 10:22:21a.m.
Ticket asignado: TK318138
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud

Solución: 30/08/2021 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: 30/08/2021 08:28:32p.m.
Tiempo total del Ticket: 00 10:06:11

Título: Reporte de consumo de ancho de banda-2021-08-31-1000_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.

Atendido por: GONZALEZ CURENO, ROGELIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 31/08/2021 10:04:50a.m.
Ticket asignado: TK318191
Medio de contacto: Correo electronico
Estado evento: Cerrado
Clasificación: Solicitud



CANAL 22

Detalle de Eventos

Solución: 31/08/2021 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: 31/08/2021 09:00:49p.m.

Tiempo total del Ticket: 00 10:55:59

Título: ModificCertificado portalproyectos.canal22.org.mx_CANAL 22

Descripción:

Solicito su ayuda para renovar el certificado SSL al portal web "https://portalproyectos.canal22.org.mx" con el siguiente NAT.

Nombre Publicado Firewall

IP Publica

WAF

IP Interna

Portal Proyectos

189.204.131.144

10.0.0.219

172.20.22.25

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



CANAL 22

Detalle de Eventos

Atendido por:	CARLOS CRUZ, ELIDETH
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	18/08/2021 11:40:14a.m.
Ticket asignado:	TK317632
Medio de contacto:	Correo electronico
Estado evento:	Abierto con Registro Relacionado
Clasificación:	Solicitud



CANAL 22

Glosario

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

Notas:

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