Contrato No.	281 de 2020		
Nombre del Contratista y/o Representante Legal	Internexa en la nube		
Nombre del Supervisor y/o Interventor	CARLOS ANDRES RUIZ ROMERO	**Teléfono / Extensión**	4322760 ext 1727
Dependencia	Dirección de Gestión de Tecnologías de Información y Comunicaciones		
Objeto del Contrato	Adquirir los Servicios de Nube Privada para cumplir su objeto misional de manera efectiva y eficiente con la ayuda de herramientas tecnológicas, a través del Acuerdos Marco de Precios reduce costos en dichos servicios		
Fecha de Inicio	1/10/2020	**Fecha de Terminación**	31/10/2022

Periodo del Informe de Actividades	**Desde**	1/07/2022	**Hasta**	30/07/2022
Adición y/o Prórroga	Adición No. 1 por la suma de $ 423.827.841,14 vigencia 2021 Adición No. 2 por la suma de $ 1.578.528.816,48 vigencia 2022			
Suspensión	NA			
Cesión	NA			

INFORME PARCIAL DE EJECUCIÓN DE OBLIGACIONES CONTRACTUALES [i]

Obligación contractual		Actividad desarrollada	Producto y/o Entregables	Alertas, inconvenientes o situaciones especiales que afectan el cumplimiento de la obligación
1	Adquirir los servicios de nube privada	Prestar el servicio de nube privada para soportar la infraestructura tecnológica de la entidad	Infraestructura de nube privada instalada	No se evidencia situaciones que afecten el cumplimiento de la obligación en el periodo reportado

Hago constar que durante el periodo reportado se adelantaron las anteriores obligaciones y/o actividades.

VBEpardo

Firma del Contratista
Fecha: 29/08/2022

BALANCE ECONÓMICO

Valor Total Contrato (Inicial + Adición)		Valor Pagado	Valor a Pagar	Saldo Liberado	Saldo por Pagar
Vigencia 2020	$543.260.652,89	$543.260.652,89	$0	$0	$0
Vigencia 2021	$3.590.891.898,14	$2.550.938.834,81	$0	$1.039.953.063,33	$0
Vigencia 2022	$2.898.138.840,48	$1.512.014.896,82	$314.854.779,79	$0	$1.071.269.163,87

La ADRES cancelará al CONTRATISTA, la suma de trescientos catorce millones ochocientos cincuenta y cuatro mil setecientos setenta y nueve con setenta y nueve centavos ($314.854.779,79)

PAGO DE SEGURIDAD SOCIAL PERSONAS NATURALES
Mes de ejecución contractual

CONCEPTO	PLANILLA No.	VALOR	PERIODO		FECHA DE PAGO
			DESDE	HASTA	
Salud	1047963635	$76.272.400	1/08/2022	31/08/2022	8/08/2022
Pensión			1/07/2022	31/07/2022	8/08/2022
ARL			1/07/2022	31/07/2022	8/08/2022

El Contratista tiene otros Contratos de Prestación de Servicios:

SI ☐ NO ☒

En la eventualidad que la Supervisión verifique que la información suministrada por el Contratista no es consistente o carece de validez, ésta deberá indicar las acciones tomadas: Realizar una breve descripción del hallazgo (Adjuntar soportes)

INFORME PARCIAL DE SUPERVISIÓN

De conformidad con el seguimiento a la ejecución del contrato, el (los) supervisor (es) certifica(n) que:

1. El (la) Contratista durante el periodo de ejecución del contrato, desarrolló y cumplió con objeto contractual, las obligaciones generales y específicas, presentó y entregó los productos y/o informes establecidos en el Contrato o Convenio en mención.

2. Apruebo los informes, productos y demás documentos presentados y entregados por el (la) Contratista durante el periodo mencionado en desarrollo de las obligaciones pactadas en el Contrato o Convenio en mención.

3. A la fecha no existen causales de incumplimiento de las obligaciones contractuales que demanden actuaciones conminatorias o sancionatorias por parte de la Administración.

OBSERVACIONES	NA
ANEXOS	1. Comprobante del pago de los Aportes respectivos al Sistema de Seguridad Social Integral en Salud y Pensiones y/o Aportes Parafiscales por parte del Contratista. 2. Soportes contractuales cargados en la sección 7 del contrato electrónico (Formato comprimido). 3. Cuenta de cobro o factura, según el Régimen sea Simplificado o Común. Factura electrónica de venta No. FEUT-155 4. En caso de primer pago debe aportar: a. Los soportes relacionados en el formato de deducciones para efectos de retención en la fuente.

En constancia, firmo:

CARLOS ANDRES RUIZ ROMERO
Supervisor (es)/Interventor (es)

En constancia, el presente documento se entiende aprobado por las partes una vez el usuario supervisor del contrato efectue la aprobacion respectiva en la plataforma de SECOP II.

Lugar y Fecha: Bogotá, D. C., 5/09/2022

[i] Incluir las obligaciones específicas pactadas en el Contrato y/o Convenio.

INTERNEXA EN LA NUBE
NIT 901.334.455-1
CL 26 69 63 ED TORRE 26 P 6 OF 601
Tel: 3153363561
Bogotá - Colombia
aldemar.marin@enlanube.com.co

Factura electrónica de venta
No. FEUT-155

Señores	Administradora de los Recursos del Sistema General de Seguridad Social en Salud		
NIT	901.037.916-1	**Teléfono**	3305000
Dirección	CR 13 32 76	**Ciudad**	Bogotá - Colombia

Fecha y hora Factura	
Generación	26/08/2022, 18:06
Expedición	26/08/2022, 18:06
Vencimiento	25/09/2022

Ítem	Descripción	Cantidad	Vr. Unitario	Impto. Cargo	Vr. Total
1	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Intermedio - Nube privada - SQL Server 2012 R2 o superior - PaaS/M- Cantidad: 7 (Línea No. 1)	1.00	31,306,242.69	0 %	30,210,524.20
2	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Intermedio - Nube privada - SQL Server 2012 R2 o superior - PaaS/M- Cantidad: 7 (Línea No. 1)	1.00	8,944,640.77	0 %	8,631,578.34
3	npn03--PaaS - SQL Sobre Windows - Oro - Alta - Servidor de Uso Estandar - Nube privada - SQL Server 2012 R2 o superior - PaaS/M- Cantidad: 25 (Línea No. 3)	1.00	56,388,697.56	0 %	54,415,093.15
4	npn03--PaaS - Internet Information 20.0 Server - Oro - Alta - Servidor de Uso Estandar - Nube privada - PaaS/M- Cantidad: 24 (Línea No. 4)	1.00	17,139,165.23	0 %	16,539,294.45
5	npn03--PaaS - Tomcat - Oro - Alta - Servidor de Uso Estandar - Nube privada - 6.0x o superior - PaaS/M- Cantidad: 13 (Línea No. 5)	1.00	9,276,925.97	0 %	8,952,233.56
6	npn03--PaaS - Active Directory - Oro - Alta - Servidor de Uso Básico - Nube privada - PaaS/M- Cantidad: 3 (Línea No. 6)	1.00	1,367,493.07	0 %	1,319,630.81
7	npn03--IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - Nube Privada - Capacidad: 200TB a <500TB - FC >= 8 Gbps - SSD - RAID: 6 - IOPS READ 72000 / WRITE 30000 - GB/Mes - Cantidad: 495000 (Línea No. 7)	1.00	51,029,323.00	0 %	49,243,296.69
8	npn03--IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - Nube Privada - Capacidad: 200TB a <500TB - FC >= 8 Gbps - SSD - RAID: 6 - IOPS READ 72000 / WRITE 30000 - GB/Mes - Cantidad: 300000 (Línea No. 8)	1.00	28,550,862.78	0 %	27,551,582.58
9	npn03--IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - Nube Privada - Capacidad: 200TB a <500TB - FC >= 8 Gbps - SSD - RAID: 6 - IOPS READ 72000 / WRITE 30000 - GB/Mes - Cantidad: 300000 (Línea No. 9)	1.00	28,550,862.78	0 %	27,551,582.58
10	npn03--Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 2 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M- Cantidad: 3 (Línea No. 10)	1.00	5,279,078.23	19 %	6,097,335.35
11	npn03--Alojamiento de infraestructura - Housing/Colocation - Punto de Red Adicional - Oro - 1 Gbps - Upra/M- Cantidad: 1 (Línea No.11)	1.00	1,180,264.63	19 %	1,363,205.65
12	npn03--IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 50TB a <100TB - Cintas LTO2, LTO4, LTO G5, LTO6 LTO7 y LTO8 - Diaria - GB/Mes - Cantidad: 54000 (Línea No. 12)	1.00	2,215,762.62	19 %	2,636,757.52
13	npn03--Alojamiento de infraestructura - Housing - Cross Conexión - Oro - Puntos de red: 2 - Capacidad de energía: 1 KVA - Capacidad en unidades: 4 U - Rack/M- Cantidad: 3 (Linea No. 13)	1.00	1,180,264.62	0 %	1,138,955.36
14	npn03--IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 50TB a <100TB - Cintas LTO2, LTO4, LTO G5, LTO6 LTO7 y LTO8 - Semanal - GB/Mes - Cantidad: 77000 (Línea No. 14)	1.00	3,159,513.37	0 %	3,048,930.40
15	npn03--IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 50TB a <100TB - Cintas LTO2, LTO4, LTO G5, LTO6 LTO7 y LTO8 - Semanal - GB/Mes - Cantidad: 100000 (Línea No. 15)	1.00	4,103,264.12	0 %	3,959,649.88
16	npn03--IaaS almacenamiento - Backup de Datos - Alta - Mes Capacidad: 50TB a <100TB - Almacenamiento SAN - Diario - GB/Mes - Cantidad: 54000 (Linea No. 16)	1.00	3,969,546.91	0 %	3,830,612.77

Ítem	Descripción	Cantidad	Vr. Unitario	Impto. Cargo	Vr. Total
17	npn03--IaaS almacenamiento - Backup de Datos - Alta - Mes Capacidad: 50TB a <100TB - Almacenamiento SAN - Diario - GB/Mes - Cantidad: 54000 (Linea No. 17)	1.00	3,236,704.93	0 %	3,123,420.26
18	npn03--IaaS almacenamiento - Backup de Datos - Alta - Mes Capacidad: 50TB a <100TB - Almacenamiento SAN - Diario - GB/Mes - Cantidad: 54000 (Linea No. 17)	1.00	732,841.98	0 %	707,192.51
19	pn03--IaaS almacenamiento - Backup de Datos - Alta - Mes Capacidad: 50TB a <100TB - Almacenamiento SAN - Semanal - GB/Mes - Cantidad: 77000 (Linea No. 18)	1.00	5,660,279.85	0 %	5,462,170.06
20	npn03--IaaS almacenamiento - Backup de Datos - Alta - Mes Capacidad: 50TB a <100TB - Almacenamiento SAN - Semanal - GB/Mes - Cantidad: 77000 (Linea No. 19)	1.00	5,660,279.85	0 %	5,462,170.06
21	npn03--IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 100TB a <200TB - Almacenamiento SAN - Mensual - GB/Mes - Cantidad: 100000 (Línea No. 20)	1.00	7,351,012.79	0 %	7,093,727.34
22	npn03--IaaS almacenamiento - Backup de Datos - Alta - Capacidad: 100TB a <200TB - Almacenamiento SAN - Mensual - GB/Mes - Cantidad: 100000 (Línea No. 21)	1.00	7,351,012.79	0 %	7,093,727.34
23	npn03--IaaS almacenamiento - Custodia de Copias de Seguridad - Cintas LTO2, LTO4, LTO G5, LTO6 LTO7 y LTO8 - Med/M- Cantidad: 60 (Línea No. 22)	1.00	2,119,376.50	19 %	2,447,879.86
24	npn03--IaaS almacenamiento - Custodia de Copias de Seguridad - Cintas LTO2, LTO4, LTO G5, LTO6 LTO7 y LTO8 - Med/M- Cantidad: 60 (Línea No. 23)	1.00	2,119,376.50	19 %	2,522,058.04
25	npn03--Servicios Complementarios - Experto Master - Región 1 - Hora/M- Cantidad: 20 (Línea No. 27)	1.00	226,066.97	0 %	218,154.63
26	npn03--Servicios Complementarios - Experto Master en Base de Datos MSSQLServer - Región 1 - Hora/M- Cantidad: 20 (Línea No. 28)	1.00	226,066.97	0 %	218,154.63
27	npn03--Servicios Complementarios - Arquitecto Master en Computación en la Nube - Región 1 - Hora/M- Cantidad: 20 (Línea No. 29)	1.00	489,811.77	0 %	472,668.36
28	npn03--Servicios Complementarios - Arquitecto Master en Computación en la Nube - Región 1 - Hora/M- Cantidad: 20 (Línea No. 29)	1.00	4,301,577.11	0 %	4,151,021.91
29	npn03--IaaS Procesamiento - Balanceador de Carga Baja Capacidad - Oro - Hosting Físico - Sesiones Capa L4 (entre 1.6 y 14 Millones) - RAMentre 8GB y 32GB - U_Mes - Cantidad: 1 (Línea No. 31)	1.00	1,750,316.15	0 %	1,689,055.08
30	npn03--IaaS Seguridad - Web Aplication Firewall - Media Capacidad - Oro - Hosting Fisico - Desempeñ0 WAF (Mbps) - 500-Mes Cantidad 1 (Línea No. 32)	1.00	1,418,770.11	0 %	1,369,113.16
31	npn03--IaaS Seguridad - Monitoreo y Correlación - Oro - Eventos por segundo (EPS) - por unidad - entre 251 y 500 - Und - Cantidad: 1 (Línea No. 33)	1.00	27,031.22	19 %	31,221.06
32	npn03--IaaS Seguridad - Monitoreo y Correlación - Oro - Eventos por segundo (EPS) - por unidad - entre 251 y 500 - Und - Cantidad: 1 (Línea No. 34)	1.00	13,515,610.84	19 %	15,610,530.52

Total Bruto	309,828,044.68
IVA 19%	5,026,735.11
Retefuente 3.5%	10,692,251.68
ReteIVA 15%	754,010.27
ReteICA 9.66	2,992,938.91
Total a Pagar	**300,415,578.93**

Total items: 32

Valor en Letras:
Trescientos millones cuatrocientos quince mil quinientos setenta y ocho pesos m/cte con noventa y tres cent.

Condiciones de Pago:
Crédito - Cuota No. 001 vence el 2022-09-25 por $ 300,415,578.93

Observaciones:
Nota: Periodo Servicio Julio de 2022
Miembro de la Unión Temporal Internexa en la Nube:
1. Internexa SA NIT: 811.021.654
2. Infraestructura Virtual SAS NIT: 900.486.933
Por favor tener en cuenta el siguiente porcentaje de participación de los miembros de la UT en el presente documento:
1. Internexa SA 8.74%

1. Internexa SA 8,74%
2 Infraestructura Virtual SAS 91,26%
Internexa SA es autoretenedor según Resolución No. 12584 de Diciembre 17 /2002

Porcentaje de participación de los miembros:

Infraestructura Virtual SAS - NIT 900.486.933 - 91.26%
Internexa SA - NIT 811.021.654 - 8.74%

A esta factura de venta aplican las normas relativas a la letra de cambio (artículo 5 Ley 1231 de 2008). Con esta el Comprador declara haber recibido real y materialmente las mercancías o prestación de servicios descritos en este título - Valor. **Número Autorización 18764024102857 aprobado en 20220114 prefijo FEJT desde el número 1 al 200 Vigencia: 18 Meses**

Responsable de IVA - Actividad Económica 6110 Actividades de telecomunicaciones alámbricas Tarifa 9.66

CUFE: 462f461f43cd541262bdc6a785db745fa4ad81c83904879af28572d3ce0e7adfe509abc2987f943e5a5c7084cf65e83a

Transacción Aprobada

Su planilla ha sido enviada y pagada con éxito. Por favor imprima este comprobante como soporte del envío y pago de su planilla.

Información de la Planilla Pagada

Nit de comercio Operador de Información	900097333-9
Razón Social del Operador de Información	SIMPLE S.A.
Descripción	Pago de SuAporte
Fecha	2022-08-08, 04:11:19 PM
Periodo de Cotización Otros Riesgos	julio de 2022
Periodo de Cotización Para Salud	agosto de 2022
Empresa	INFRAESTRUCTURA VIRTUAL SAS
NIT	NI 900486933
Código Sucursal (Nombre)	( )
Referencia de Pago/ Número Planilla	1047963635
Tipo de Planilla	E
Número Transacción Bancaria/ CUS	1593834500
Banco	(1001) - BANCO DE BOGOTA
Valor	$ 76.272.400
Estado de la Transacción	Aprobada
Dirección IP de Origen	www.simple.co

Nit	Código	Administradora	Número Afiliados	Valor sin Mora	Total Intéreses Mora
N800224808	230301	PORVENIR	16	$ 10.819.300	$ 0
N800229739	230201	PROTECCION FONDO DE PENSIONES OBLIGATORIAS	5	$ 9.650.100	$ 0
N900336004	25-14	COLPENSIONES	7	$ 7.561.400	$ 0
N800227940	231001	COLFONDOS	11	$ 7.604.600	$ 0
N800253055	230901	OLD MUTUAL SKANDIA	4	$ 5.549.100	$ 0
N900156264	EPS037	NUEVA EPS S.A.	1	$ 80.000	$ 0
N800251440	EPS005	ENTIDAD PROMOTORA DE SALUD SANITAS S.A.	11	$ 6.935.200	$ 0
N830003564	EPS017	ENTIDAD PROMOTORA DE SALUD FAMISANAR LIMITADA CAFAM-COLSUBSIDIO	9	$ 2.738.200	$ 0
N901021565	ESSC18	CMRC RECAUDO FOSYGA-EMSSANAR E.S.S	1	$ 44.000	$ 0
N805001157	EPS018	ENTIDAD PROMOTORA DE SALUD SERVICIO OCCIDENTAL DE SALUD S.A. S.O.S.	1	$ 69.200	$ 0
N830113831	EPS001	ALIANSALUD EPS S.A.	2	$ 3.440.000	$ 0
N800130907	EPS002	SALUD TOTAL S.A. ENTIDAD PROMOTORA DE SALUD	3	$ 1.688.200	$ 0
N800088702	EPS010	EPS SURA	9	$ 2.391.800	$ 0
N860066942	EPS008	COMPENSAR ENTIDAD PROMOTORA DE SALUD	5	$ 731.100	$ 0
N901037916	MIN002	ADMINISTRADORA DE LOS RECURSOS SS ADRES	1	$ 1.744.800	$ 0
N800226175	14-25	RIESGOS PROFESIONALES COLMENA S.A COMPANIA DE SEGUROS DE VIDA	44	$ 1.242.000	$ 0
N890500675	CCF36	CAJA DE COMPENSACION FAMILIAR DEL ORIENTE COLOMBIANO COMFAORIENTE	1	$ 168.000	$ 0
N890303208	CCF57	COMFANDI	6	$ 891.500	$ 0
N860066942	CCF24	CAJA DE COMPENSACION FAMILIAR COMPENSAR	36	$ 7.876.200	$ 0
N899999034	PASENA	SENA	10	$ 2.019.200	$ 0
N899999239	PAICBF	INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR	10	$ 3.028.500	$ 0
		SubTotales:		$ 76.272.400	$ 0
		Total a Pagar:			$ 76.272.400

compensar | miplanilla.com

REPORTE RESUMEN DE PAGO

Información básica de la planilla

Empresa:	INTERNEXA S.A.	**NIT:**	811021654
Tipo Planilla:	E	**Periodo liquidación Pensiones:**	julio 2022
Sucursal o Dependencia:	PRINCIPAL	**Periodo liquidación Salud:**	agosto 2022
Número de Radicación:	60531531	**Total a pagar:**	$762,895,000
Fecha de vencimiento:	02/08/2022	**Total de empleados:**	229
Fecha de Pago:	29/07/2022	**Número de Administradoras:**	22

Detalles del pago

Razón social recaudo:	Compensar OI	**Nit recaudo:**	9998600669427
Descripción:	MiPlanilla.com Pago Proteccion Social	**Medio de Pago:**	Pago Electronico por PSE
Banco:	BANCOLOMBIA	**Número Autorización:**	1575624008
Estado de la transacción:	Transacción aprobada		

Código	NIT	Administradoras	Num. Afiliados	*Número de incapacidad por riesgos laborales	Valor descontado en incapacidad y/o licencia	Total Pagado
14-25	800226175	Riesgos Profesionales Colmena	229		$0	$29,203,600
230201	800229739	Proteccion (ING + Proteccion)	97		$0	$146,264,200
230301	800224808	Porvenir	29		$0	$42,017,600
230901	800253055	FONDO DE PENSIONES OBLIGATORIAS SKANDIA	11		$0	$19,053,100
231001	800227940	Colfondos	17		$0	$26,444,300
25-14	900336004	Administradora Colombiana de Pensiones -	66		$0	$116,301,700
CCF04	890900841	Comfama Caja de Compensacion Fliar	164		$0	$58,660,600
CCF07	890101994	Comfamiliar del Atlantico Caja de Compensacion	2		$0	$950,300
CCF24	860066942	Compensar Caja de Compensacion Fliar	52		$0	$20,302,200
CCF40	890201578	Comfenalco Santander Caja de Compensacion	1		$0	$1,416,100
CCF57	890303208	Comfamiliar Andi Comfandi Caja de	2		$0	$1,098,400
EPS001	830113831	ALIANSALUD EPS S.A.	5		$0	$3,839,400
EPS002	800130907	Salud Total EPS	7		$0	$7,750,100
EPS005	800251440	Sanitas EPS	37		$0	$38,496,800
EPS008	860066942	Compensar EPS	13		$0	$16,745,600
EPS010	800088702	EPS Sura	159		$0	$147,900,000
EPS017	830003564	Famisanar EPS Cafam Colsubsidio	2		$0	$1,348,700

Código	NIT	Administradoras	Num. Afiliados	*Número de incapacidad por riesgos laborales	Valor descontado en incapacidad y/o licencia	Total Pagado
EPS018	805001157	Servicio Occidental de Salud S.A. S.O.S EPS	1		$0	$192,000
EPS037	900156264	Nueva Promotora de Salud - Nueva EPS	5		$0	$2,066,000
ESSC62	900935126	ASMET SALUD EPS SAS	1		$0	$125,000
PAICBF	899999239	ICBF Instituto Colombiano de Bienestar Familiar	140		$0	$49,629,900
PASENA	899999034	SENA	140		$0	$33,089,400
						$762,895,000

***Si descontó incapacidades o notas crédito debe informar a la administradora correspondiente los descuentos.**

Financial Planner Consulting S.A.S

CERTIFICACION DE PAGOS DE SEGURIDAD SOCIAL Y APORTES PARAFISCALES
ARTÍCULO 50 DE LA LEY 789 DE 2002

Para dar cumplimiento a lo previsto en el artículo 50 de la ley 789 de 2002, el suscrito **VÍCTOR JULIO GUTIÉRREZ ACERO** identificado con la cédula de ciudadanía número 79.203.201 expedida en Soacha y tarjeta profesional 73.020 - T, Revisor Fiscal de la sociedad **INFRAESTRUCTURA VIRTUAL SAS,** Identificada con NIT No. **900.486.933 - 7** se permite certificar que la mencionada sociedad ha realizado los pagos de seguridad social (pensión, salud y riesgos laborales) y aportes parafiscales correspondientes a las nóminas de los últimos seis (06) meses, por lo tanto a la fecha se encuentra a paz y salvo por concepto de aportes a la seguridad social integral y aportes parafiscales.

La anterior certificación se expide para efectos de dar cumplimiento al artículo 50 de la Ley 789 de 2002, la ley 797 de 2003, el decreto 510 de 2003, y el art. 41 de la ley 80 de 1993 modificado por el art. 1150 de 2008.

Dado en Bogotá a los diez (10) días del mes de agosto del año 2022.

VÍCTOR JULIO GUTIÉRREZ ACERO
Revisor Fiscal Delegado por Financial Planner Consulting SAS.
C.C. 79.203.201 de Soacha
T.P 73.020 - T

Building a better working world

MA-2219-22

Señores
Internexa S.A.
Medellín Antioquia

Fui nombrado Revisor Fiscal de Internexa S.A. identificada con NIT: 811.021.654 para el periodo comprendido entre 1 de enero a 31 de diciembre de 2022. Actualmente me encuentro desarrollando los procedimientos necesarios para cumplir con mis funciones como Revisor Fiscal.

Los registros contables por el periodo comprendido entre el 1 de febrero al 31 de julio de 2022, no auditados, de las subcuentas 2424017700 – "Acreedores Aportes Fondos Pensionales -Pagos", 2424027700 – "Aportes Seguridad Social -Pagos", 2424027800- "Acreedores Riesgo Profesional-Pagos", 2511247700- "Cajas de Compensación", 2490507700- "Acreedores Aportes ICBF, SENA" y las planillas de autoliquidación de aportes, incluyen el siguiente pago de aportes a las entidades respectivas así:

Mes de causación	Número de planilla Integrada de Liquidación de Aporte (PILA)	Valor Pagado	Mes de pago	Estado de la planilla
Febrero 2022	57068989	$ 964,658,300	Marzo 2022	Pagado
Marzo 2022	57729275	653,695,600	Abril 2022	Pagado
Abril 2022	58377477	733,114,600	Abril 2022	Pagado
Mayo 2022	59194534	668,095,100	Mayo 2022	Pagado
Junio 2022	59806127	643,695,000	Julio 2022	Pagado
Julio 2022	60531531	$ 762,895,000	Julio 2022	Pagado

Las planillas integradas de liquidación evidencian el pago de dichos aportes por el período antes mencionado.

La información financiera, contable, extracontable y tributaria es responsabilidad de la Administración de la Compañía.

No estoy enterado de situaciones que impliquen cambios significativos a la información anteriormente indicada,

Building a better working world

Esta comunicación se emite a solicitud de la Administración de la Compañía en cumplimiento del artículo 50 de la Ley 789 de 2002 y no debe ser utilizada para ningún otro propósito.

FERNEY ALONSO CANO VARGAS

Firmado digitalmente por FERNEY ALONSO CANO VARGAS
Fecha: 2022.08.05 12:26:07 -05'00'

Ferney Alonso Cano Vargas
Revisor Fiscal
Tarjeta Profesional 243764-T
Designado por Ernst & Young Audit S.A.S. TR-530

Medellín, Antioquia
5 de agosto de 2022

Tabla 15. Casos reportados en el mes julio 2022

INFORME DE CASOS REGISTRADOS - SERVICIOS DE DATACENTER

ADRES - Administradora de los Recursos del Sistema General de Seguridad Social en Salud

PERÍODO: 01/07/2022 - 31/07/2022

No.	Tipo	Fecha Inicio	Hora Inicio	Canal	Solicitante	Asunto	Fecha de cierre	Hora cierre	Responsable	Solución	Indisponibilidad servicio	Tiempo indisponibilidad	% Disponibilidad
220611129	Solicitud de servicio	1/07/2022	3:08 p. m.	Correo	Enlanube	Lentitud procesamiento BDPCOM01	5/07/2022	2:03 p.m.	Javier Orejarena	Buenas tardes, sobre este asunto ya había respondido la semana pasada, pero grosso modo la respuesta es que no ha habido cambios físicos en la infraestructura y por lo tanto se recomienda ejecutar el tunning de las bases de datos de acuerdo con la guía de tunning de la herramienta Microsoft SQL DTA.	NO	0	100,00%
220711161	Solicitud de servicio	5/07/2022	11:02 a.m.	Correo	Enlanube	Validar WAF en DC	6/07/2022	12:07 p.m.	Juan Manuel Rojas	Se adjunta archivo con la información solicitada,	NO	0	100,00%
220711207	Solicitud de servicio	8/07/2022	3:39 p.m.	Correo	Enlanube	Configuración WAF DC	12/07/2022	2:06 p.m.	Juan Manuel Rojas	El día de ayer y el día de hoy se realizaron sesiones por el aplicativo teams con los ingenieros Fabian y Wilmer de ADRES para efectuar la actividad solicitada con respecto a los protocolos TLS 1.0 y 1.1, Quedando estos protocolos deshabilitados para las siguientes Server Policy	NO	0	100,00%
220711218	Solicitud de servicio	12/07/2022	9:01 a.m.	Correo	Enlanube	APPRECDT01 - 192.168.60.48	12/07/2022	9:51 a.m.	Mario Merlini	Revisando el Host en el cual esta corriendo la maquina virtual, encontramos una utilizacion adecuada de los recursos. En CPU queda libre el 74%, en Memoria queda libre el 54%.	NO	0	100,00%
220711230	Solicitud de servicio	12/07/2022	3:02 p.m.	Correo	Enlanube	WAF para iservicios.adres.gov.co referente a Cross-site Scripting	29/07/2022	10:20 a.m.	Juan Manuel Rojas	12/07/2022 4:23 p.m. Se realizó sesión de validación y configuraciones. 21/07/2022 4:49 p.m. El día martes a las 3:00 pm y el día de hoy a las 8:00 am se realizan sesiones por teams con los ingenieros Wilmer y Fabian de ADRES en donde se realizan configuraciones en el WAF para el servicio iservicios con respecto a mitigar el cross-site Scripting (XSS), Una vez realizados estos cambios en el WAF, personal de ADRES indica realizaran pruebas de funcionamiento para validar que el servicio no se vea afectado por los mismos, ingenieros Wilmer y Fabian indican agendaran otra sesión para continuar con la actividad y validar si se realiza esta configuración para los demás servicios, 29/07/2022 10:20 a.m. El día de ayer (28 de Julio) a las 2:00 pm y el día de hoy a las 9:00 am se realizan sesiones con personal de ADRES (ingenieros Fabian y Wilmer) por el aplicativo teams, en donde se ejecutan configuraciones y pruebas con respecto a Cross-site Scripting en el servicio iservicio, una vez realizado esto, el cliente realizara pruebas de funcionamiento y dependiendo del comportamiento del servicio se ejecutarán nuevas configuraciones de ser requeridas, Se está a la espera de la programación de una nueva sesión por parte del personal de ADRES para continuar.	NO	0	100,00%
220711232	Solicitud de servicio	12/07/2022	3:46 p.m.	Correo	Enlanube	Antivirus SOPHOS	13/07/2022	9:09 p.m.	Martin Bulla	Se creó una nueva política NO_RT_SCANNING para prevenir el escaneo en tiempo real de los archivos locales y remotos por parte del antivirus en las máquinas APPSER02 y APPRECDT01 respectivamente.	NO	0	100,00%
1085	Solicitud de servicio	25/07/2022	10:55 a.m.	Correo	Enlanube	Restauración Data SFTP APPMFT01	25/07/2022	2:33 p.m.	Mario Merlini	Buenas tardes Ingenieros, los archivos solicitados para restauración ya se encuentran en las carpetas requeridas.	NO	0	100,00%
1131	Solicitud de servicio	28/07/2022	8:59 a.m.	Correo	Enlanube	ALERTA Cliente ADRES: El Nodo APPGW se encuentra en estado Down	28/07/2022	2:28 p.m.	Mario Merlini	Buenas tardes Ingenieros, revisando la maquina del asunto, podemos indicar que la maquina no tiene ningún evento de reinicio sobre la plataforma de virtualización, se ha monitoreado y se ha podido evidenciar que la maquina deja internamente de responder. No tengo usuario y password para reiniciar la maquina adecuadamente desde el sistema operativo. Es necesario que el proveedor del softare revise el comportamiento de la máquina.	NO	0	100,00%
1137	Solicitud de servicio	28/07/2022	2:52 p.m.	Correo	Enlanube	Eliminación maquina APPMOV01	28/07/2022	3:46 p.m.	Javier Orejarena	Buenas tardes, correcto, procederemos a su borrado después de 11:59 pm del día de hoy.	NO	0	100,00%
1143	Solicitud de servicio	28/07/2022	3:49 p.m.	Correo	Enlanube	Aprovisionamiento de disco en servidor BDPERP01	28/07/2022	5:24 p.m.	Javier Orejarena	Buenas tardes, se aprovisionan los discos solicitados.	NO	0	100,00%

INFORME DE DISPONIBILIDAD
PaaS

ADRES - Administradora de los Recursos del Sistema General de Seguridad Social en Salud

El propósito de este documento es detallar por escrito la disponibilidad del servicio contratado para el mes de julio– 2022.

Contenido

1. DESCRIPCIÓN DEL SERVICIO

El servicio de Data Center brindado por **UT-INTERNEXA-ENLANUBE** a **Administradora de los Recursos del Sistema General de Seguridad Social en Salud (ADRES),** en el presente documento se identifican las especificaciones y disponibilidad del servicio contratado. El modelo de prestación de servicio entregado a **ADRES** es Plataforma (PaaS) bajo el modelo de implementación de Nube Privada. Servicio de Data Center principal– ITX.

Tabla 1. Información básica del proyecto

Entidad compradora		ADRES
Servicio entregado		Nube Privada
Modelo de servicio		**PaaS**
Fecha		8 de agosto 2022
UT-INTERNEXA-ENLANUBE	**Gerente de proyecto**	Abraham Ramirez Martinez
	Director Arquitectura de Soluciones	Daniel Sanchez
Representantes entidad compradora		Carlos Ruiz

1.1. INFRAESTRUCTURA O DIAGRAMA DE LA SOLUCIÓN TECNOLÓGICA

El siguiente diagrama detalla los componentes que conforman la infraestructura tecnológica que soporta el servicio de Plataforma de **ADRES**.

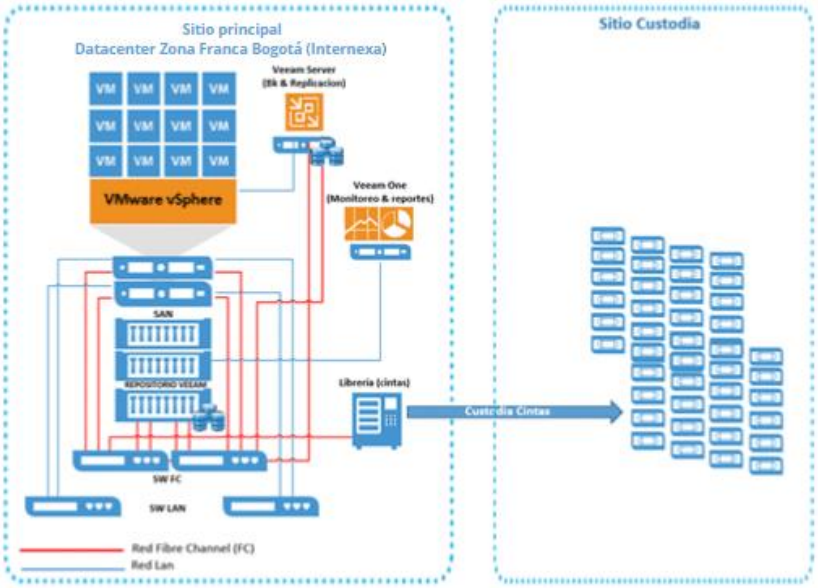


Figura 1. Infraestructura de la solución.

A continuación, se encuentra la topología actual.

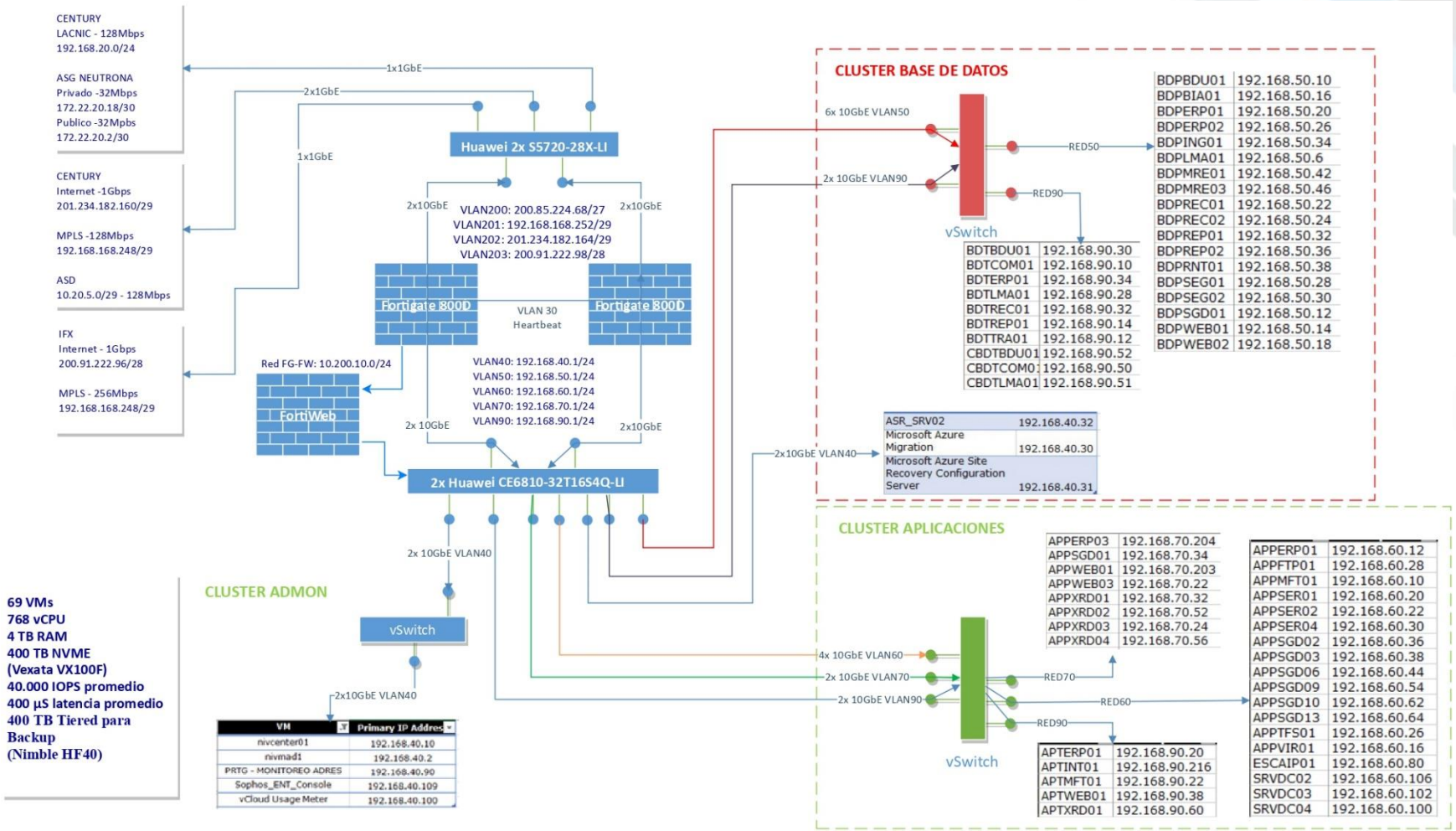


Figura 2. Topología actual

2. ESPECIFICACIONES DEL SERVICIO CONTRATADO

El servicio de Plataforma PaaS de **ADRES** esta soportado por Windows Server, donde la administración del servidor es compartida, es decir, **ADRES** es responsable de la administración de las aplicaciones que se instalen sobre la plataforma; mientras que **UT-INTERNEXA-ENLANUBE** es responsable de instalar, administrar y configurar la plataforma.

2.1. DATA CENTER PRINCIPAL

Dentro del contrato 003, se encuentran los ítems que corresponden a los servicios contratados para el datacenter principal. Estos ítems corresponden a necesidades de computo, conectividad, almacenamiento y gestión. A continuación, se explican uno a uno los servicios que conforman la infraestructura contratada por **INSFRAESTRUCTURA VIRTUAL** en el datacenter principal y la aprovisionada en este, ITX.

2.1.1. SERVIDORES

Los servicios contratados dentro del ítem cómputo o servidores se muestran en la siguiente tabla, acompañado de su ubicación dentro del anexo 1. Contrato 003 para su verificación. Una condición transversal independiente del rol del servidor es que son de tipo virtual y requiere una velocidad mínima de procesador de 2.6 Ghz.

Tabla 2. Identificación de Servicios contratados – Servidores en ITX.

Nombre del Servicio	Número del ítem. Anexo 1
SQL sobre Windows	Ítem 1-2
Internet Information Server	Ítem 3
Tomcat	Ítem 4
Active Directory	Ítem 5

Este servicio se divide según las características de cada servidor. La clasificación se da de la siguiente manera: Servidor de uso básico, estándar, intermedio, avanzado y optimizado. En seguida se realiza la identificación de los componentes dentro de cada servicio, clasificándolos por el rol y las características de cómputo requeridas para la prestación del servicio:

a. Servidores de bases de datos. SQL Server

La tabla número 3, servidores contratados por **ADRES** evidencia las características de cómputo contratadas.

Tabla 3. Servidores SQL contratados por ADRES en ITX.

Ítem	Código del servicio	Resumen del Producto	Cantidad
1	S1-IT-NP-PA-11-15	PaaS - SQL sobre Windows - Oro - Alta - **Servidor de Uso Intermedio** - Nube privada – SQL Server 2012 R2 o superior - PaaS/M	9
2	S1-IT-NP-PA-11-9	PaaS - SQL sobre Windows - Oro - Alta - **Servidor de Uso Estandar** - Nube privada - SQL Server 2012 R2 o superior - PaaS/M	25
TOTAL			34

La tabla número 4, servidores SQL aprovisionados por **UT-INTERNEXA-ENLANUBE** contiene las características de cómputo de los servidores virtuales aprovisionados.

Tabla 4. Servidores SQL aprovisionados por UT-INTERNEXA-ENLANUBE en ITX.

Total VM	VM NAME	OS according to the configuration file	vCPUs	Memory GB	NICs	Disks	Provisioned GB
1	BDPBDU01	Microsoft Windows Server 2019	32	131	1	15	16.586
2	BDPBDU02	Microsoft Windows Server 2019	32	131	1	15	16.586
3	BDPBIA01	Microsoft Windows Server 2016	16	65	1	9	10.388
4	BDPCOM01	Microsoft Windows Server 2019	32	131	2	21	42.042
5	BDPERP01	Microsoft Windows Server 2012 R2	32	131	2	9	6.456
6	BDPERP02	Microsoft Windows Server 2012 R2	32	131	2	6	3.244
7	BDPING01	Microsoft Windows Server 2012	16	32	2	5	1.587
8	BDPLMA01	Microsoft Windows Server 2019	32	131	1	13	21.802
9	BDPLMA02	Microsoft Windows Server 2019	32	131	1	13	21.802
10	BDPMRE01	Microsoft Windows Server 2016	16	32	1	9	23.586
11	BDPMRE02	Microsoft Windows Server 2019	32	131	2	11	25.753
12	BDPMRE03	Microsoft Windows Server 2016	16	32	1	10	21.374
13	BDPREC01	Microsoft Windows Server 2019	32	131	1	9	11.174
14	BDPREC02	Microsoft Windows Server 2012 R2	32	131	2	7	4.292
15	BDPREP01	Microsoft Windows Server 2012 R2	16	32	2	5	1.589
16	BDPREP02	Microsoft Windows Server 2012 R2	16	32	2	5	1.589
17	BDPSEG01	Microsoft Windows Server 2012 R2	16	32	2	5	794
18	BDPSEG02	Microsoft Windows Server 2012 R2	16	32	2	5	794
19	BDPSGD01	Microsoft Windows Server 2012 R2	32	131	1	7	7.647
20	BDPWEB01	Microsoft Windows Server 2012 R2	32	98	2	13	11.219
21	BDPWEB02	Microsoft Windows Server 2016	16	81	1	13	5.760
22	BDPRNT01	Microsoft Windows Server 2019	16	81	1	13	11.084
23	BDTBDU01	Microsoft Windows Server 2019	16	65	1	7	7.339
24	BDTCOM01	Microsoft Windows Server 2019	20	98	1	16	30.015
25	BDTERP01	Microsoft Windows Server 2012 R2	16	32	2	6	5.185
26	BDTLMA01	Microsoft Windows Server 2019	16	65	1	10	14.154
27	BDTREC01-26112021	Microsoft Windows Server 2019	16	65	2	5	8700
28	BDTREP01	Microsoft Windows Server 2016	16	32	1	6	934
29	BDTTRA01	Microsoft Windows Server 2019	16	65	1	11	14.131
30	ASR_SRV02	Microsoft Windows Server 2016	16	32	1	2	1.204
31	ESCAIP01	Microsoft Windows Server 2019	16	32	2	1	155
32	BDPREP03	Microsoft Windows Server 2019	16	32	1	2	1.277
33	UBDPREC02	Microsoft Windows Server 2019	32	131	1	7	4.358
34	UBDPSEG01	Microsoft Windows Server 2019	16	32	1	5	860
35	UBDPSEG02	Microsoft Windows Server 2019	16	32	1	5	860
36	UBDTREC01	Microsoft Windows Server 2019	16	65	1	5	8649
37	UBDTREP01	Microsoft Windows Server 2019	16	32	1	6	934
			804	2.818			

b. Servidores de Aplicaciones APP

Dentro de los servidores de aplicación tenemos Internet Information Server y Tomcat.

La tabla número 5, servidores de aplicación – Internet Information Server contratados por **ADRES** en ITX, contiene información tomada del Anexo 1 Contrato 003., allí se evidencian las características de cómputo requeridas para cada servidor contratado.

Tabla 5. Servidores de aplicación - Internet Information Server contratados por ADRES en ITX.

Ítem	Código del servicio	Resumen del Producto	Cantidad
3	S1-IT-NP-PA-1-9	PaaS - Internet Information Server - Oro - Alta - Servidor de Uso Estandar - Nube privada - PaaS/M	24
TOTAL			24

La tabla número 6, servidores de aplicación – Tomcat contratados por **ADRES** en ITX de tipo virtual, contiene información tomada del Anexo 1. Contrato 003, allí se evidencian las características de cómputo requeridas para cada servidor contratado.

Tabla 6. Servidores de Aplicación -Tomcat contratados por ADRES en ITX (Tipo virtual)

Ítem	Código del servicio	Resumen del Producto	Cantidad
4	S1-IT-NP-PA-5-9	PaaS - Tomcat - Oro - Alta - Servidor de Uso Estandar - Nube privada - 6.0x o superior - PaaS/M	14
TOTAL			14

El total de servidores de aplicación contratados son 38, como se muestra desde la tabla número 5 a la 7. Son 24 de Internet Information Server y 14 de Tomcat.

La tabla número 7, servidores de aplicación aprovisionados por **UT-INTERNEXA-ENLANUBE** contiene las características de cómputo de los servidores aprovisionados en ITX.

Tabla 7. Servidores de Aplicación aprovisionado por UT-INTERNEXA-ENLANUBE en ITX.

Total VM	VM NAME	OS according to the configuration file	vCPUs	Memory GB	NICs	Disks	Provisioned GB
1	APPERP01	Microsoft Windows Server 2012 R2	16	32	2	5	744
2	APPERP03	Microsoft Windows Server 2012 R2	16	32	2	5	860
3	APPFTP01	Microsoft Windows Server 2019	16	32	2	8	4.867
4	APPGW	Red Hat Enterprise Linux 7 (64-bit)	4	16	4	3	4.770
5	APPINT01	Microsoft Windows Server 2019	16	49	2	6	849
6	APPINT02	Microsoft Windows Server 2019	16	32	2	6	824
7	APPMFT01	Microsoft Windows Server 2019	16	65	2	13	26.119
8	APPMX	Red Hat Enterprise Linux 7 (64-bit)	4	32	2	1	1.056
9	APPSER01	Microsoft Windows Server 2019	16	32	2	6	607
10	APPSER02	Microsoft Windows Server 2019	16	32	1	23	61.297
11	APPSER04	Microsoft Windows Server 2019	16	32	2	7	6.701
12	APPSGD01	Microsoft Windows Server 2019	16	65	2	6	828
13	APPSGD02	Microsoft Windows Server 2019	16	65	2	6	2270
14	APPTFS02	Microsoft Windows Server 2019	16	32	2	3	839
15	APPSGD06	Microsoft Windows Server 2019	16	32	2	5	673
16	APPSGD07	Microsoft Windows Server 2019	16	32	2	5	673
17	APPRECDT01	Microsoft Windows Server 2019	16	32	2	3	2.425
18	APPSGD09	Microsoft Windows Server 2019	16	32	2	14	29.154
19	APPSGD10	Microsoft Windows Server 2019	16	65	2	12	37.605
20	APPSGD13	Microsoft Windows Server 2019	16	32	2	5	8.844
21	APPTFS01	Microsoft Windows Server 2019	16	32	2	6	1000
22	APPVIR01	Microsoft Windows Server 2019	16	32	1	12	24.913
23	APPWEB01	Microsoft Windows Server 2019	16	65	2	8	1.723
24	APPWEB02	Microsoft Windows Server 2019	16	65	2	6	951
25	APPWEB03	Microsoft Windows Server 2019	16	32	2	6	540
26	APPWEB_07	Microsoft Windows Server 2019	16	32	2	6	689
27	APTERP01	Microsoft Windows Server 2012 R2	16	32	2	6	999

28	APTINT01	Microsoft Windows Server 2019	16	32	2	6	660
29	APTMFT01	Microsoft Windows Server 2019	16	32	2	8	2.692
30	APTWEB01	Microsoft Windows Server 2019	16	32	1	6	923
31	APPXRD01	Ubuntu Linux	6	32	2	1	544
32	APPXRD02	Ubuntu Linux	6	32	2	1	544
33	APPXRD03N	Ubuntu Linux	16	32	1	1	544
34	APPXRD04	Ubuntu Linux	16	32	2	1	557
35	APTXRD01	Ubuntu Linux	16	32	2	1	557
36	APDFAB01	Microsoft Windows Server 2022	16	32	1	3	426
			532	1376			

c. Servidor directorio activo

La tabla número 8, servidores de Directorio Activo contratados por **ADRES** contiene información tomada del Anexo 1., allí se evidencian las características de cómputo contratadas para este ítem.

Tabla 8. Servidores Directorio Activo contratados por ADRES en ITX.

Ítem	Código del servicio	Resumen del Producto	Cantidad
5	S1-IT-NP-PA-2-3	PaaS - Active Directory - Oro - Alta - Servidor de Uso Básico - Nube privada - PaaS/M	3
TOTAL			3

La tabla número 9, servidores de directorio activo aprovisionados por **UT-INTERNEXA-ENLANUBE** contiene las características de cómputo de los servidores aprovisionados en ITX.

Tabla 9. Servidores de Directorio Activo aprovisionado por UT-INTERNEXA-ENLANUBE en ITX

Total VM	VM NAME	OS according to the configuration file	vCPUs	Memory GB	NICs	Disks	Provisioned GB
1	SRVDC02	Microsoft Windows Server 2019	8	16	2	5	385
2	SRVDC03	Microsoft Windows Server 2019	8	16	2	5	385
3	SRVDC04	Microsoft Windows Server 2019	4	8	2	5	262

2.1.2. ALMACENAMIENTO

Servicios de Infraestructura de almacenamiento de la información, que le permiten a **ADRES** crear áreas para archivar y procesar datos.

Tabla 10. Identificación de servicios contratados - Almacenamiento

Nombre del Servicio	Número del ítem. Anexo 1
Almacenamiento SAN Alto Rendimiento	6-7
Copias de seguridad	10-16

a. Almacenamiento máquinas virtuales

Como servicios de almacenamiento de máquinas virtuales **ADRES** contrato Almacenamiento SAN Alto Rendimiento. Este servicio consiste en una red de área de almacenamiento que interconecta y comparte un grupo de recursos de almacenamiento con sistemas de cómputo (servidores de datos, web, aplicaciones, bases de datos).

- **Almacenamiento SAN Alto Rendimiento**

El tipo de disco de almacenamiento es unidades de disco duro de estado sólido, SSD. El protocolo de transferencia de datos está basado en canal de fibra, FC.
La tabla 11 muestra los detalles del servicio de SAN Alto Rendimiento contratado por **ADRES** en ITX.

Tabla 11. Almacenamiento SAN Alto Rendimiento contratado por ADRES en ITX

Ítem	Código del servicio	Resumen del Producto	Cantidad	Características				Observaciones
				Capacidad	Velocidad FC	RAID	IOPS	
6	S1-IT-NP-IA-3-267	IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - NA - Nube Privada - .GB/Mes -	495000	200 a 500 TB	≥ 8 Gbps	6	READ: 72.000 WRITE: 30.000	Topología SAN: Switched Fabric 16 Gbps
7	S1-IT-NP-IA-3-267	IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - NA - Nube Privada - .GB/Mes -	300000	200 a 500 TB	≥ 8 Gbps	6	READ: 72.000 WRITE: 30.000	Topología SAN: Switched Fabric 16 Gbps

La figura 2 muestra la información básica de identificación del Almacenamiento Huawei Dorado 5000 V3.

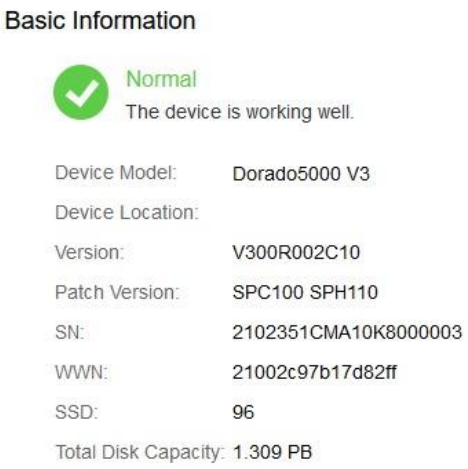


Figura 3. Información de identificación del Almacenamiento aprovisionado.

Dentro del almacenamiento Huawei actualmente a nivel de producción se están consumiendo 615 TB

La tabla 12, Almacenamiento SAN Alto Rendimiento aprovisionado por **UT-INTERNEXA-ENLANUBE** en ITX contiene las LUN presentadas del Almacenamiento a los dos cluster de vmware, reservado para los servidores de producción.

Tabla 12. Almacenamiento SAN Alto Rendimiento aprovisionado por UT-INTERNEXA-ENLANUBE en ITX. SSD

Name	Type	# VMs	Provisioned MB
APDFAB01_0001	VMFS	1	427.573
APPMFT01_0001	VMFS	1	7.295.542
APPMFT01_0002	VMFS	1	6.243.391
APPMFT01_0003	VMFS	1	12.585.522
APPSER01_0001	VMFS	1	2.098.227
APPSER02_0001	VMFS	1	14.932.852
APPSER02_0002	VMFS	1	14.681.204

APPSER02_0003	VMFS	1	14.681.183
APPSER02_0004	VMFS	1	7.571.058
APPSER02_0005	VMFS	1	7.342.280
APPSER04_0001	VMFS	2	8.426.148
APPSGD09_0001	VMFS	1	12.616.941
APPSGD09_0002	VMFS	1	11.608.165
APPSGD09_0003	VMFS	1	4.932.678
APPSGD10_0001	VMFS	1	7.722.248
APPSGD10_0002	VMFS	1	10.486.822
APPSGD10_0003	VMFS	1	5.243.956
APPSGD10_0004	VMFS	1	14.156.866
APPSGD10_0005	VMFS	1	2.426.167
APPVIR01_0001	VMFS	1	8.389.620
APPVIR01_0002	VMFS	1	8.389.688
APPVIR01_0003	VMFS	1	8.138.867
ASR_0001	VMFS	3	4.020.060
BDPBIA01N_0001	VMFS	1	952.942
BDPBIA01N_0002	VMFS	1	1.050.058
BDPBIA01N_0003	VMFS	1	2.098.651
BDPBIA01N_0004	VMFS	1	2.098.651
BDPBIA01N_0005	VMFS	1	2.098.651
BDPBIA01N_0006	VMFS	1	2.098.651
BDPCOM01N_0001	VMFS	1	132.394
BDPCOM01N_0002	VMFS	1	2.098.151
BDPCOM01N_0003	VMFS	1	2.098.151
BDPCOM01N_0004	VMFS	1	2.098.151
BDPCOM01N_0005	VMFS	1	2.098.152
BDPCOM01N_0006	VMFS	1	2.098.156
BDPCOM01N_0007	VMFS	1	2.098.150
BDPCOM01N_0008	VMFS	1	2.098.150
BDPCOM01N_0009	VMFS	1	2.098.149
BDPCOM01N_0010	VMFS	1	2.098.151
BDPCOM01N_0011	VMFS	1	2.098.150
BDPCOM01N_0012	VMFS	1	2.098.151
BDPCOM01N_0013	VMFS	1	2.098.156
BDPCOM01N_0014	VMFS	1	3.115.016
BDPCOM01N_0015	VMFS	1	4.195.311
BDPCOM01N_0016	VMFS	1	3.165.334
BDPCOM01N_0017	VMFS	1	2.098.150
BDPCOM01N_0018	VMFS	1	2.098.668
BDPCOM01N_0019	VMFS	1	2.098.668
BDPERP01_0001	VMFS	0	1.524
BDPERP01N_0001	VMFS	1	329.512
BDPERP01N_0002	VMFS	1	296.364
BDPERP01N_0003	VMFS	1	68.012
BDPERP01N_0004	VMFS	1	1.050.068
BDPERP01N_0005	VMFS	1	1.050.058
BDPERP01N_0006	VMFS	1	1.050.058
BDPERP01N_0007	VMFS	1	2.622.974
BDPERP02_0001	VMFS	1	3.245.834
BDPLMA01N_0001	VMFS	0	1.490
BDPLMA01N_0002	VMFS	0	1.490
BDPLMA01N_0003	VMFS	0	1.490

BDPLMA01N_0004	VMFS	0	1.490
BDPLMA01N_0005	VMFS	0	1.490
BDPLMA01N_0006	VMFS	0	1.490
BDPLMA01N_0007	VMFS	0	1.490
BDPLMA01N_0008	VMFS	0	1.490
BDPLMA01N_0009	VMFS	0	1.490
BDPLMA01N_0010	VMFS	0	1.490
BDPLMA01N_0011	VMFS	0	1.490
BDPLMA02_0001	VMFS	0	1.490
BDPMRE01_0001	VMFS	1	11.014.824
BDPMRE01_0002	VMFS	1	12.583.821
BDPMRE02_0001	VMFS	1	11.284.124
BDPMRE02_0002	VMFS	1	12.374.283
BDPMRE02_0003	VMFS	1	2.098.651
BDPMRE03_0002	VMFS	1	8.389.681
BDPMRE03N_0001	VMFS	1	2.501.290
BDPMRE03N_0002	VMFS	1	4.195.837
BDPMRE03N_0003	VMFS	1	4.195.837
BDPMRE03N_0004	VMFS	0	1.524
BDPMRE03N_0005	VMFS	0	1.524
BDPMRE03N_0006	VMFS	1	2.098.685
BDPREC01_0001	VMFS	3	1.861.029
BDPREC01N_0001	VMFS	1	1.738.441
BDPREC01N_0002	VMFS	1	2.098.651
BDPREC01N_0003	VMFS	1	2.098.655
BDPREC01N_0004	VMFS	1	2.099.147
BDPREC01N_0005	VMFS	1	2.098.660
BDPREC01N_0006	VMFS	1	1.050.058
BDPREC02N_0001	VMFS	1	689.770
BDPREC02N_0002	VMFS	1	1.050.058
BDPREC02N_0003	VMFS	1	1.050.058
BDPREC02N_0004	VMFS	1	525.770
BDPREC02N_0005	VMFS	1	1.050.058
BDPSGD01_0001	VMFS	1	1.357.493
BDPSGD01_0002	VMFS	1	2.098.651
BDPSGD01_0003	VMFS	1	2.098.671
BDPSGD01_0004	VMFS	1	2.098.651
BDPWEB01_0001	VMFS	1	11.220.507
BDPWEB02_0001	VMFS	2	16.845.929
BDTERP01_0001	VMFS	1	5.187.972
BDTREC01_0001	VMFS	0	2.360.025
BDTREC01_0002	VMFS	0	2.098.651
BDTREC01_0003	VMFS	0	2.098.651
BDTREC01_0004	VMFS	0	2.098.651
BDTREP01_0001	VMFS	0	411.315
BDTREP01_0002	VMFS	0	263.600
BDTREP01_0003	VMFS	0	263.600
BDTTRA01N_0001	VMFS	1	14.133.855
CBDTBDU01_0001	VMFS	1	7.341.423
CBDTCOM01_0001	VMFS	1	657.024
CBDTCOM01_0002	VMFS	1	2.098.651
CBDTCOM01_0003	VMFS	1	2.098.651
CBDTCOM01_0004	VMFS	1	2.098.651

CBDTCOM01_0005	VMFS	1	1.050.075
CBDTCOM01_0006	VMFS	0	1.490
CBDTCOM01_0007	VMFS	1	2.098.651
CBDTCOM01_0008	VMFS	1	2.098.651
CBDTCOM01_0009	VMFS	1	2.098.651
CBDTCOM01_0010	VMFS	1	2.098.651
CBDTCOM01_0011	VMFS	1	2.098.651
CBDTCOM01_0012	VMFS	1	1.050.075
CBDTCOM01_0013	VMFS	1	2.098.651
CBDTCOM01_0014	VMFS	0	1.490
CBDTCOM01_0015	VMFS	1	4.195.837
CBDTCOM01_0016	VMFS	1	4.195.837
CBDTCOM01_0017	VMFS	0	1.490
CBDTLMA01_0001	VMFS	1	8.914.278
CBDTLMA01_0002	VMFS	1	5.245.119
datastore1	VMFS	0	1.453
Datastore-esx01	VMFS	0	12.138
Datastore-esx02	VMFS	0	12.138
Datastore-esx03	VMFS	0	12.138
Datastore-esx05	VMFS	0	12.138
Datastore-esx06	VMFS	0	12.138
Datastore-esx07	VMFS	0	12.138
Datastore-esx08	VMFS	0	12.138
Datastore-esx09	VMFS	0	12.138
Datastore-esx10	VMFS	0	12.138
DS_APPS_0001	VMFS	28	40.159.068
DS_APPS_0002	VMFS	2	10.895.553
DS_APPS_0003	VMFS	3	1.768.916
DS_BD_0001	VMFS	8	7.480.131
DS_BD_0003	VMFS	2	5.571.073
DS_BD_0004	VMFS	1	8.701.094
DS_HUAWEI_ADMON	VMFS	10	3.479.338
UBDPBDU01_0001	VMFS	1	1.908.469
UBDPBDU01_0002	VMFS	1	2.098.651
UBDPBDU01_0003	VMFS	1	2.098.651
UBDPBDU01_0004	VMFS	1	2.098.651
UBDPBDU01_0005	VMFS	1	1.050.058
UBDPBDU01_0006	VMFS	1	1.050.058
UBDPBDU01_0007	VMFS	1	1.050.058
UBDPBDU01_0008	VMFS	1	1.050.058
UBDPBDU01_0009	VMFS	1	1.050.058
UBDPBDU01_0010	VMFS	1	1.050.058
UBDPBDU01_0011	VMFS	1	1.050.058
UBDPBDU01_0012	VMFS	1	1.051.129
UBDPBDU02_0001	VMFS	1	1.907.589
UBDPBDU02_0002	VMFS	1	2.098.651
UBDPBDU02_0003	VMFS	1	2.098.651
UBDPBDU02_0004	VMFS	1	2.098.651
UBDPBDU02_0005	VMFS	1	1.050.058
UBDPBDU02_0006	VMFS	1	1.050.058
UBDPBDU02_0007	VMFS	1	1.050.058
UBDPBDU02_0008	VMFS	1	1.050.058
UBDPBDU02_0009	VMFS	1	1.050.058

UBDPBDU02_0010	VMFS	1	1.050.060
UBDPBDU02_0011	VMFS	1	1.050.058
UBDPBDU02_0012	VMFS	1	1.050.058
UBDPLMA01_0001	VMFS	1	832.225
UBDPLMA01_0002	VMFS	1	2.098.651
UBDPLMA01_0003	VMFS	1	2.098.668
UBDPLMA01_0004	VMFS	1	2.098.651
UBDPLMA01_0005	VMFS	1	2.098.651
UBDPLMA01_0006	VMFS	1	2.098.651
UBDPLMA01_0007	VMFS	1	2.098.651
UBDPLMA01_0008	VMFS	1	2.098.651
UBDPLMA01_0009	VMFS	1	2.098.651
UBDPLMA01_0010	VMFS	1	2.098.657
UBDPLMA01_0011	VMFS	1	2.098.651
UBDPLMA02_0001	VMFS	1	832.336
UBDPLMA02_0002	VMFS	1	2.098.651
UBDPLMA02_0003	VMFS	1	2.098.668
UBDPLMA02_0004	VMFS	1	2.098.651
UBDPLMA02_0005	VMFS	1	2.098.651
UBDPLMA02_0006	VMFS	1	2.098.651
UBDPLMA02_0007	VMFS	1	2.098.651
UBDPLMA02_0008	VMFS	1	2.098.651
UBDPLMA02_0009	VMFS	1	2.098.651
UBDPLMA02_0010	VMFS	1	2.098.652
UBDPLMA02_0011	VMFS	1	2.098.651
			615.970.415

Tabla 13. Almacenamiento SAN aprovisionado por UT-INTERNEXA-ENLANUBE en ITX para BDPCOM02 (Máquina física)

Name	Health ...	Running ...	Use Type	Capa...	Owning Storage Pool	Mapping	Data Protection Capacity	Application Type
BDPCOM02_0001	Normal	Online	Internal	2.000 TB	POOL01	Mapped	1.673 TB	SQL_Server_OLAP&OLTP
BDPCOM02_0002	Normal	Online	Internal	2.000 TB	POOL01	Mapped	18.475 GB	SQL_Server_OLAP&OLTP
BDPCOM02_0003	Normal	Online	Internal	2.000 TB	POOL01	Mapped	21.217 GB	SQL_Server_OLAP&OLTP
BDPCOM02_0004	Normal	Online	Internal	2.000 TB	POOL01	Mapped	26.913 GB	SQL_Server_OLAP&OLTP
BDPCOM02_0005	Normal	Online	Internal	2.000 TB	POOL01	Mapped	66.795 GB	SQL_Server_OLAP&OLTP
BDPCOM02_0006	Normal	Online	Internal	2.000 TB	POOL01	Mapped	336.288 GB	SQL_Server_OLAP&OLTP
BDPCOM02_0007	Normal	Online	Internal	2.000 TB	POOL01	Mapped	1.458 TB	SQL_Server_OLAP&OLTP
BDPCOM02_0008	Normal	Online	Internal	2.000 TB	POOL01	Mapped	546.964 GB	SQL_Server_OLAP&OLTP
BDPCOM02_0009	Normal	Online	Internal	2.000 TB	POOL01	Mapped	1.539 TB	SQL_Server_OLAP&OLTP
BDPCOM02_0010	Normal	Online	Internal	2.000 TB	POOL01	Mapped	448.008 GB	SQL_Server_OLAP&OLTP
BDPCOM02_0011	Normal	Online	Internal	2.000 TB	POOL01	Mapped	75.273 MB	SQL_Server_OLAP&OLTP
BDPCOM02_0012	Normal	Online	Internal	2.000 TB	POOL01	Mapped	64.468 MB	SQL_Server_OLAP&OLTP
BDPCOM02_0013	Normal	Online	Internal	2.000 TB	POOL01	Mapped	79.226 MB	SQL_Server_OLAP&OLTP
BDPCOM02_0014	Normal	Online	Internal	2.000 TB	POOL01	Mapped	31.761 GB	SQL_Server_OLAP&OLTP
BDPCOM02_0015	Normal	Online	Internal	4.000 TB	POOL01	Mapped	3.709 TB	SQL_Server_OLAP&OLTP
BDPCOM02_0016	Normal	Online	Internal	3.000 TB	POOL01	Mapped	2.794 TB	SQL_Server_OLAP&OLTP
BDPCOM02_0017	Normal	Online	Internal	2.000 TB	POOL01	Mapped	0.000 MB	SQL_Server_OLAP&OLTP

b. Almacenamiento copias de seguridad

La información a respaldar son los Datos de los servidores de producción, copias completas de los datos y copias técnicas de duplicación de datos para la eliminación de información redundante. La periodicidad del Backup es diaria, semanal y mensual, se realiza su ejecución en horas no hábiles. Finalmente, el tamaño de respaldo contratado por **ADRES** es igual a 462 TB.

Los detalles del servicio contratado por **ADRES** se muestran en la tabla 13, Copias de seguridad de datos contratados por **ADRES**.

Tabla 14. Almacenamiento Copias de seguridad de datos contratadas por ADRES en ITX.

Ítem	Código del servicio	Resumen del Producto	Cantidad	Características		Observaciones
				Capacidad	Medio	
10	S1-IT-NP-IA-6-55	IaaS almacenamiento – Backup de datos- Alta – Diaria - GB/Mes	54000	50 a <100 TB	Cinta LTO6	Copias de seguridad de datos: DATA y VMs.
11	S1-IT-NP-IA-6-58	IaaS almacenamiento – Backup de datos- Alta – Semanal - GB/Mes	77000	50 a <100 TB	Cinta LTO6	Copias de seguridad de datos: DATA y VMs.
12	S1-IT-NP-IA-6-70	IaaS almacenamiento – Backup de datos- Alta – Mensual - GB/Mes	100000	100 a <200 TB	Cinta LTO6	Copias de seguridad de datos: DATA y VMs.
13	S1-IT-NP-IA-6-57	IaaS almacenamiento – Backup de datos- Alta – Diaria - GB/Mes	54000	50 a <100 TB	Disco duro externo	-
14	S1-IT-NP-IA-6-60	IaaS almacenamiento – Backup de datos- Alta – Semanal - GB/Mes	77000	50 a <100 TB	Disco duro externo	-
15	S1-IT-NP-IA-6-72	IaaS almacenamiento – Backup de datos- Alta – Mensual - GB/Mes	100000	100 a <200 TB	Disco duro externo	-

La tabla 14, Copias de seguridad de datos aprovisionadas por **UT-INTERNEXA-ENLANUBE** contiene los detalles del almacenamiento copias de seguridad aprovisionado.

Tabla 15. Almacenamiento Copias de seguridad de datos a CINTA aprovisionado por UT-INTERNEXA-ENLANUBE en ITX.

Librería HPE MSL con dos drives FC, capacidad para 24 cintas LTO7				
Backup Servers	**Tape Server Name**	**Type**	**Connected Tape Library**	**Throttling**
192.168.40.80				
	WIN-TF08DTFKMLN	Physical	HPE MSL G3 Series 6.90	Disable

La figura número 3 muestra las LUN de almacenamiento presentadas al servidor de backup. Las cuatro (4) primeras unidades de 128 TB cada una, las cuales se usan para la toma de backups, la unidad 5 para las copias de los backups y las retenciones mensuales.

Name	Health Status	Running Status	Capacity	Owning Storage Pool
BACKUP0001	Normal	Online	128.000 TB	POOL01
BACKUP0002	Normal	Online	128.000 TB	POOL01
BACKUP0003	Normal	Online	128.000 TB	POOL01
BACKUP0004	Normal	Online	128.000 TB	POOL01
BACKUP0005	Normal	Online	256.000 TB	POOL01

Figura 4. Almacenamiento Copias de seguridad de datos aprovisionado por UT-INTERNEXA-ENLANUBE en ITX.

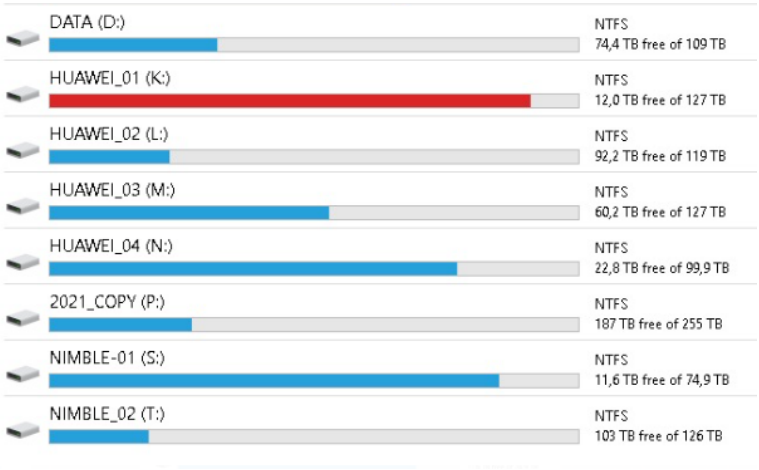
3. DISPONIBILIDAD DEL SERVICIO

3.1. CONSUMO BACK UP

3.1.1. BACKUP DISCO REPOSITORIOS VEEAM

En el almacenamiento Huawei se tienen actualmente seis (6) repositorios y en el almacenamiento Nimble dos (2) repositorios de backup a disco, para el alojamiento de las tareas de backup diarias, semanales y mensuales. Las siguientes graficas detallan el consumo de backup a disco en estos repositorios (consumo 474,6 TB), políticas diarias y semanales.

Figura 5. Consumo de back up Repositorios Veeam



Repositorio	Tamaño uso [TB]
DATA	34,6
HUAWEI_01	115,0
HUAWEI_02	26,8
HUAWEI_03	66,8
HUAWEI_04	77,1
2021_COPY	68,0
NIMBLE_01	63,3
NIMBLE_02	23,0
TOTAL	**474,6**

3.1.2. BACKUP A CINTA

En el anexo 2, acta entrega cintas está el detalle de los archivos de backups en cinta (LTO7) correspondientes al mes de julio 2022.

3.2. CONSUMO DE COMPUTO (CPU Y RAM)

3.2.1. CLUSTER APLICACIONES

Las figuras 7 y 8 muestran el consumo de CPU y Memoria, respectivamente en el Cluster de Aplicaciones para el mes de julio 2022.

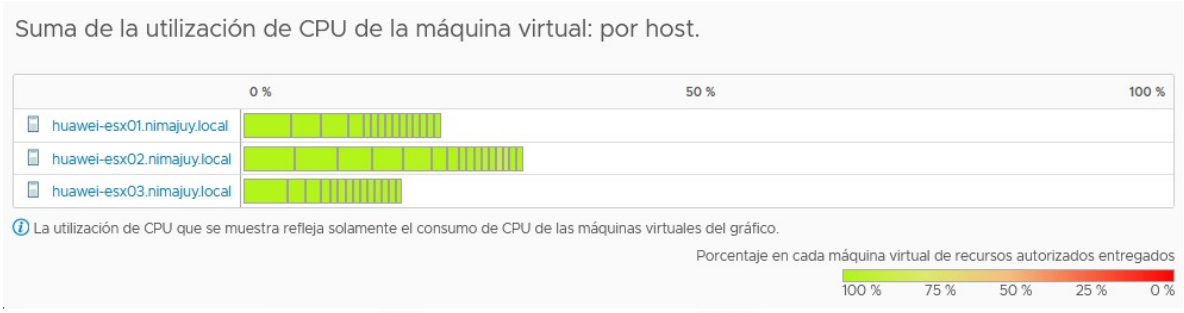


Figura 6. Consumo de CPU en Cluster de Aplicaciones

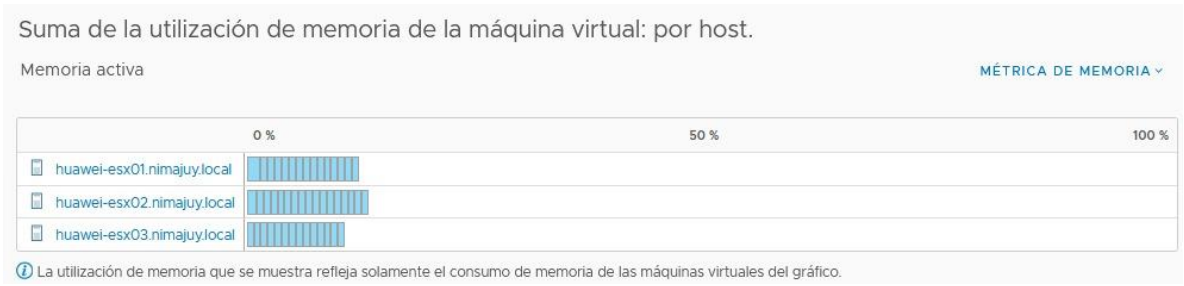


Figura 7. Consumo de memoria en Cluster de Aplicaciones.

3.2.2. CLUSTER BASE DE DATOS

Las figuras 9 y 10 muestran el consumo de CPU y Memoria respectivamente, en el Cluster de Base de datos para el mes de julio 2022.

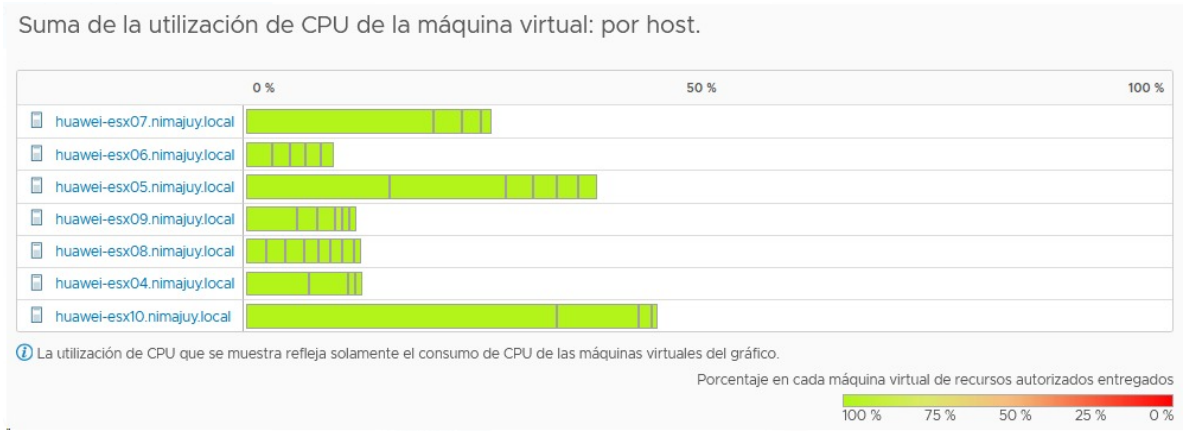


Figura 8. Consumo CPU en el Cluster de Base de datos.

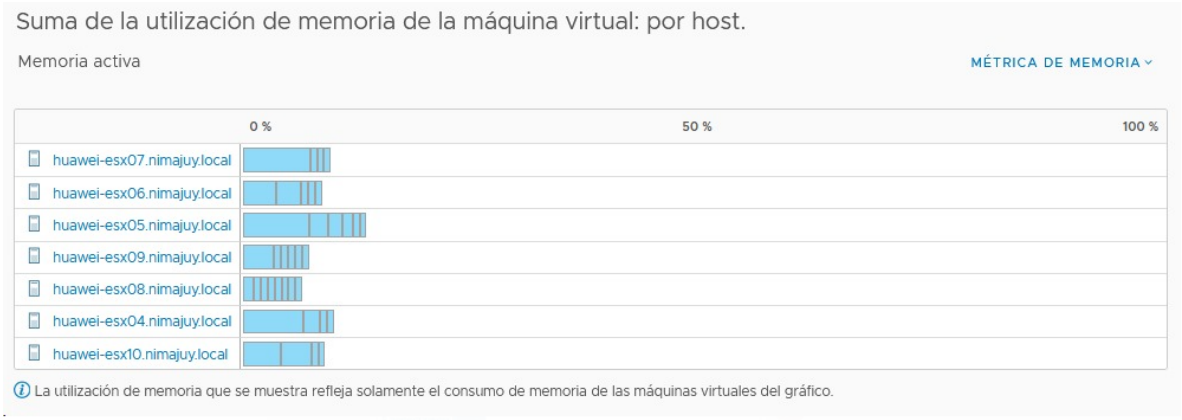


Figura 9. Consumo de Memoria en el Cluster de Base de datos.

3.3. ESCANEO DE SEGURIDAD

Se tiene establecido un control semanal sobre la plataforma con un escaneo programado con SOPHOS de los servidores de la ADRES- Por diseño de la plataforma el escaneo se realiza sobre los ítems establecidos en la política y se realiza sobre todas las maquinas asociadas a la misma simultáneamente, en caso de encontrar malware, PUAs (Potentially Unwanted Application), virus, anomalías etc, el Endpoint intentara remediar esto automáticamente e independientemente del resultado de la operación envía correo al administrador de la consola.

3.4. CASOS REPORTADOS

Los casos reportados se clasifican según su tipo, si causan una interrupción en el servicio como incidente de lo contrario solicitud de servicio.

La tabla 16 evidencia los casos registrados en el mes de julio y su clasificación.

Tabla 16. Casos registrados en el mes de julio 2021. Se envía en archivo anexo 4.

Para el cálculo del porcentaje de disponibilidad del servicio se emplea la siguiente ecuación:

$$Disponibilidad = \left(1 - \frac{Ti}{D * 24horas * 60minutos}\right) * 100\%$$

Donde:

$$Ti = Tiempo\ de\ indisponibilidad\ en\ minutos$$

$$D = Número\ de\ días\ en\ el\ mes\ contratado$$

Aplicando la ecuación de disponibilidad se obtiene que para el mes de julio el porcentaje de disponibilidad de servicio fue de 100%.

$$Disponibilidad = \left(1 - \frac{0}{31 * 24horas * 60minutos}\right) * 100\% = 100\%$$

3.4.1. DISPONIBILIDAD ITX

Tabla 17. Disponibilidad por ítem- ITX

Código del servicio	Producto	Servidor	Indisponibilidad	Disponibilidad (%)	Descripción
S1-IT-NP-PA-11-15	PaaS - SQL sobre Windows - Oro - Alta - Servidor de Uso Intermedio - Nube privada – SQL Server 2012 R2 o superior - PaaS/M			100,00	
S1-IT-NP-PA-11-9	PaaS - SQL sobre Windows - Oro - Alta - Servidor de Uso Estandar - Nube privada - SQL Server 2012 R2 o superior - PaaS/M			100,00	
S1-IT-NP-PA-1-9	PaaS - Internet Information Server - Oro - Alta - Servidor de Uso Estandar - Nube privada - PaaS/M			100,00	
S1-IT-NP-PA-5-9	PaaS - Tomcat - Oro - Alta - Servidor de Uso Estandar - Nube privada - 6.0x o superior - PaaS/M			100,00	
S1-IT-NP-PA-2-3	PaaS - Active Directory - Oro - Alta - Servidor de Uso Básico - Nube privada -PaaS/M			100,00	
S1-IT-NP-IA-3-267	IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - NA - Nube Privada - .GB/Mes			100,00	
S1-IT-NP-IA-3-267	IaaS almacenamiento - Almacenamiento SAN Alto Rendimiento - Oro - Alta - NA - Nube Privada - .GB/Mes			100,00	
S1-IT-NP-IA-6-55	IaaS almacenamiento – Backup de datos- Alta – Diaria - GB/Mes			100,00	
S1-IT-NP-IA-6-58	IaaS almacenamiento – Backup de datos- Alta – Semanal - GB/Mes			100,00	
S1-IT-NP-IA-6-70	IaaS almacenamiento – Backup de datos- Alta – Mensual - GB/Mes			100,00	
S1-IT-NP-IA-6-57	IaaS almacenamiento – Backup de datos- Alta – Diaria - GB/Mes			100,00	
S1-IT-NP-IA-6-60	IaaS almacenamiento – Backup de datos- Alta – Semanal - GB/Mes			100,00	
S1-IT-NP-IA-6-72	IaaS almacenamiento – Backup de datos- Alta – Mensual - GB/Mes			100,00	

SOC - INFORME DE JULIO DE 2022

Soporte EnLaNube

soporte@enlanube.com.co

monitoreo.cliente@enlanube.com.co

Tel: 5085603 – 018005184539

CONTENIDO

1. OBJETIVO

Presentar ante ADRES un resumen detallado del monitoreo obtenidos de la herramienta FSIEM, donde podremos ver la disponibilidad de los activos de seguridad, los incidentes de seguridad, el uso y desempeño de la herramienta y finalmente las consideraciones y recomendaciones a tener en cuenta para la mejora continua.

2. DESARROLLO

FSIEM es un correlacionador de eventos que nos permite obtener información útil sobre potenciales amenazas de seguridad de las redes críticas de negocio, a través de la estandarización de datos y priorización de amenazas, esto es posible mediante un monitoreo y análisis centralizado de datos de seguridad, obtenidos desde múltiples sistemas que hacen parte del esquema de seguridad de la compañía, tales como aplicaciones antivirus, firewalls y soluciones de prevención de intrusiones.

3. DEFINICIONES

- **Inappropriate Website access**

Network IPS o Security Gateway o Firewall detecta el acceso inapropiado al sitio web

- **Tunneled traffic detected**

Network IPS detecta tráfico tunelizado

- **Large Inbound Transfer From Outside My Country**

Detecta una transferencia entrante grande (más de 2 MB en 10 minutos) desde un destino externo que está fuera de mi país. La regla está escrita para Estados Unidos y es posible que deba ajustarse para otros países.

- **Stealth Scan**

Detecta escaneos usando una herramienta como NMap, Satan, Saint, Nikto, Nessus, etc.

- **System Exploit Detected by Network IPS**

Detecta un exploit detectado por IPS (p. ej., desbordamiento de búfer, escalada de privilegios) precedido opcionalmente por un reconocimiento

- **Inappropriate Website access: High volume**

Detecta un acceso inapropiado excesivo al sitio web desde la misma dirección IP de origen: excesivo se define por (más de 10 intentos en 1 hora)

- **Multiple IPS Detected Scans From Same Src**

Detecta múltiples escaneos IPS desde la misma IP de origen en un corto período de tiempo.

- **Inbound cleartext password usage detected**

Detecta el uso entrante de protocolos que usan contraseñas de texto claro, por ejemplo, FTP, Telnet, POP

- **Distributed DoS Attack detected by NIPS**

Detecta ataques de denegación de servicio distribuidos de alta gravedad en servidores o dispositivos de red. Estos ataques pueden lanzarse desde servidores dispersos geográficamente, lo que dificulta la defensa contra ellos.

- **Missing specific performance metric from a device:**

Detecta que un FortiSIEM no ha recibido una métrica de rendimiento específica de un dispositivo durante un período de tiempo configurado. Esto indica que (a) el sistema FortiSIEM tiene un problema de recopilación/entrega de métricas de monitoreo de rendimiento en un módulo específico o (b) hay un problema de conectividad entre el dispositivo y FortiSIEM o (c) hay un problema de conectividad dentro de la nube de FortiSIEM.

- **Server Down: No Ping Response**

Detecta que un dispositivo no responde al ping: se pierden 10 de cada 10 paquetes de ping: el host está inactivo o hay un problema de enrutamiento

- **WMI Service Unavailable**

Detecta que el servicio WMI no está disponible

- **Auto Service Stopped**

Detecta que se detuvo un servicio que se ejecutaba automáticamente. Actualmente esto funciona para servidores Windows y se detecta a través de WMI.

- **Server Degraded: Lossy Ping Response**

Detecta un host con una respuesta de ping degradada: más del 50 % de pérdida de paquetes y más de 100 ms de tiempo de respuesta promedio

- **Sudden Decrease in Reported Events From A Host**

Detecta que un dispositivo de informes de repente informa menos eventos. El promedio actual durante la ventana de tiempo de una hora es menos de 3 veces la desviación estándar y también un 50% menos que la media estadística

- **No performance metrics from a device**

Se activa cuando el Monitor de rendimiento es crítico para TODOS los trabajos de un dispositivo monitoreado, Se borra cuando el Monitor de rendimiento está normal para todos los trabajos desde ese dispositivo

- **Server Disk Latency Warning**

Detecta que la latencia de E/S del disco del servidor ha alcanzado un nivel crítico (superior a 50 milisegundos) en función de 2 lecturas sucesivas en un intervalo de 10 minutos

- **Server Disk Latency Critical**

Detecta que la latencia de E/S del disco del servidor ha alcanzado un nivel de advertencia (entre 20 y 50 mseg) en base a 2 lecturas sucesivas en un intervalo de 10 minutos

- **Sudden Increase in System CPU Usage**

Detecta un aumento repentino del 50 % en los tiempos de respuesta de WMI durante una ventana de tiempo de 30 minutos

- **High process CPU: Server**

Detecta un uso elevado de la CPU por parte de una aplicación de servidor sobre la base de 3 mediciones consecutivas en un período de 15 minutos

- **Server CPU Warning**

Detecta que la CPU del servidor ha alcanzado un nivel de advertencia (entre 75% y 85% basado en 2 lecturas sucesivas en un intervalo de 10 minutos)

- **Server CPU Critical**

Detecta que la CPU del servidor ha alcanzado un nivel crítico (superior al 85 % según 2 lecturas sucesivas en un intervalo de 10 minutos)

- **Server Installed Software Change**

Detecta instalación de software en servidores windows

- **Successful VPN Logon From Outside My Country**

Los atacantes sin conocimiento previo de las credenciales legítimas dentro del sistema o del entorno pueden adivinar las contraseñas para intentar acceder a las cuentas. Sin conocer la contraseña de una cuenta, un adversario puede optar por adivinar sistemáticamente la contraseña utilizando un mecanismo repetitivo o iterativo.

- **Large Outbound Transfer To Outside My Country**

Detecta el bloqueo de la cuenta causado por fallas de inicio de sesión excesivas. Cabe recordar que esta regla ha presentado varias personalizaciones y está en proceso de cambio.

- **Successful VPN Logon From Outside My Country**

Detecta conexiones hacia las VPN SSL e IPSEC desde IP publicas fuera de Colombia.

- **Mirai.Botnet**

Mirai es un malware de la familia de las botnets destinada a infectar los equipos conformantes del IoT. El objetivo principal de este malware es la infección de routers y cámaras IP.

- **FortiGate ips malicious url**

Trafico que está siendo bloqueado por un Fortigate porque coincide con una URL maliciosa en la lista de URL maliciosas de Prevención de intrusiones.

- **Gh0st.Rat.Botnet**

Es un troyano de acceso remoto utilizado por atacantes para controlar los equipos infectados, originalmente atribuidos a grupos en China.

- **Bladabindi.Botnet**

Es un malware de tipo troyano que infecta ordenadores con sistema operativo Windows con el objetivo de ejecutar programas de información del usuario o ejecutar procesos maliciosos.

- **Sudden User Location Change**

Detecta cambio de ubicación para un usuario inviable en el periodo de tiempo. Esto puede indicar una credencial robada.

4. DISPONIBILIDAD DE RECURSOS

4.0 Disponibilidad Plataforma

A continuación, observamos que el equipo colector ha estado activo durante los últimos 316 días y el equipo Servidor en un tiempo de operación desde los últimos 85 días.

Nombre	Direccion IP	Rol de Módulo	Tiempo de actividad	Estado de Salud
ELNFSS.ENLANUBE.COM.CO	10.99.93.120	Supervisor	85d 16h	Normal

Organización	Nombre	Direccion IP	Estado	Tiempo de actividad	Estado de Salud
Adres	CollectorAdres	10.90.54.10	up	316d 6m	Normal

Ilustración 1 Uptime de equipos FortiSIEM.

4.1 Dispositivos integrados por protocolo

Las siguientes son la CMDB de dispositivos que se encuentran integrados y su estatus al 30 de julio del 2022.

Nombre	IP	Tipo de Dispositivo	Estado	Descubierto	Metodo
AdresFSCo	10.90.54.10	CentOS Linux	Approved	Sep 20 2021, 12:57:53 PM	LOG
APPINT01	192.168.60.2	Windows Server 2019	Approved	Oct 08 2021, 03:32:29 PM	SNMP, WMI, PING
APPWEB01	192.168.70.201	Windows Server 2019	Approved	Oct 08 2021, 03:35:14 PM	SNMP, WMI, PING
FortiGate-600E	192.168.40.1	Fortinet FortiOS	Approved	Oct 01 2021, 03:13:43 PM	LOG
WAF-Adres	10.200.10.254	Fortinet FortiOS	Approved	Oct 06 2021, 11:03:03 AM	LOG

Ilustración 2 CMDB de equipos durante el mes de julio 2022.

4.2 Dispositivos por tiempo de disponibilidad

Las siguientes métricas son suministradas por los dispositivos que actualmente tienen integrados los protocolos de SNMP, por esta razón no aparecen los 5 dispositivos del cliente ADRES integrados a la solución de FORTISIEM, sin embargo, los equipos continúan siendo monitorizados por los demás métodos como Syslog y WMI, Se observa que ningún dispositivo presento una alta indisponibilidad por lo cual se cuenta con un SLA de 100%.

Host Name	Host IP	Current Uptime	Total Downtime	Achieved Uptime (SLA)
APPINT01	192.168.60.2	40d 22h	0	100
APPWEB01	192.168.70.201	39d 20h	0	100

Ilustración 3 Top disponibilidad de equipos durante el mes de julio 2022.

5. USO DE COMPONENTES

5.0 Uso de licenciamiento

Del licenciamiento habilitado para el cliente ADRES de una tasa de eventos mínima de 0,02EPS y un máximo de hasta 397 EPS, en promedio diariamente se están utilizando 96,65 EPS generado por los 4 dispositivos integrados.

Rank	License Attribute	Allowed (per License)	Current Usage
1	Total EPS	300	see below
2	Devices	Not Specified	4
3	Valid Time	CollectorAdres: undefined - undefined	CollectorAdres: expiration time not specified
4	Linux Agent	Not Specified	0
5	Windows Agent	Not Specified	0
6	FINS	Not Specified	0

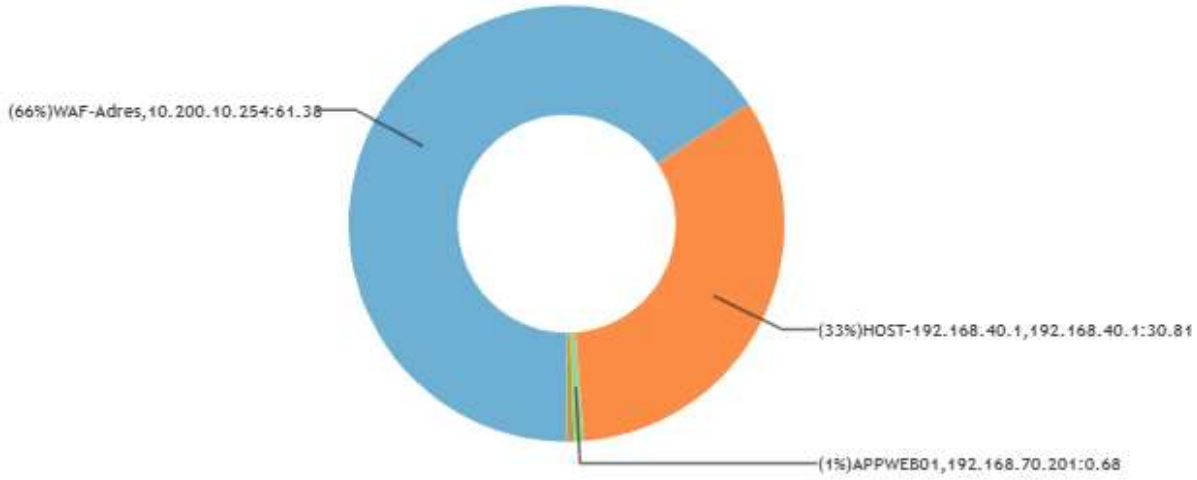
Rank	Organization ID	Reporting IP	AVG(Event Rate)	MAX(Event Rate)	MIN(Event Rate)
1	2001	10.90.54.10	96.65	397.46	0.02

Ilustración 4 Uso de licenciamiento durante el mes de julio 2022.

5.1 Dispositivos por tasa de evento

La tasa de eventos recibido en promedio por segundo por cada uno de los dispositivos integrados a la solución, los equipos que se reflejan en dicha imagen con direccionamiento 10.90.54.10 y 10.99.93.120 corresponden a los equipos Colector y Supervisor respectivos de la solución de Fortisiem.

Para los dispositivos que se encuentran con un valor promedio de 0 en el AVG (Event Rate) son dispositivos que no están generando eventos por segundo sino que por el contrario generan eventos cada x cantidad de segundos.



Reporting Device	Reporting IP	AVG(Event Rate)
WAF-Adres	10.200.10.254	61.38
HOST-192.168.40.1	192.168.40.1	30.81
APPWEB01	192.168.70.201	0.68
APPINT01	192.168.60.2	0.47
HOST-138.91.123.30	138.91.123.30	0.02
AdresFSCo	10.90.54.10	0
HOST-10.99.93.120	10.99.93.120	0
HOST-10.90.54.10	10.90.54.10	0

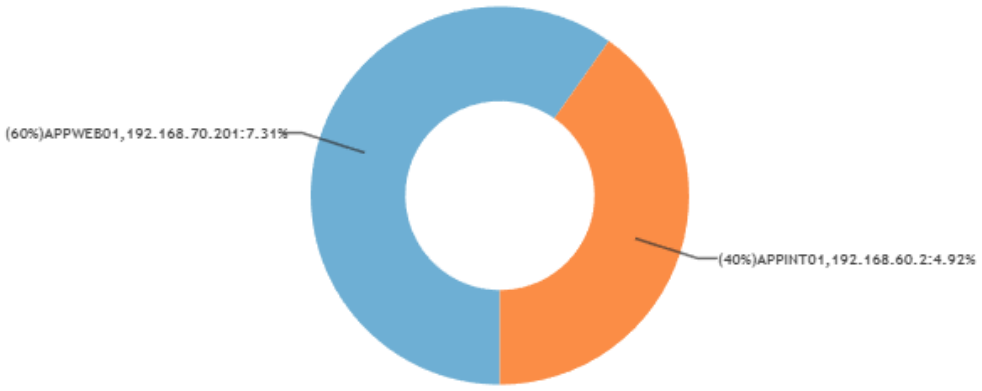
Ilustración 5 Tasa de eventos por dispositivos durante el mes de julio 2022.

6. RENDIMIENTO

A continuación, se proporciona un resumen detallado del performance (CPU y Memoria) de los dispositivos sincronizados en el FortiSIEM.

6.0 CPU

A continuación, se observa el porcentaje de CPU de los dispositivos:



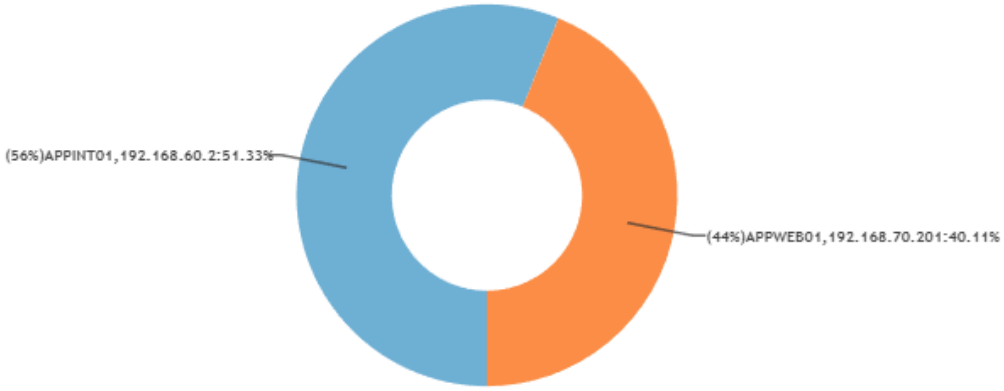
Host Name	Host IP	AVG(CPU Util)	MAX(CPU Util)	MIN(CPU Util)
APPWEB01	192.168.70.201	7.31%	70.19%	0.50%
APPINT01	192.168.60.2	4.92%	35.06%	0.06%

Ilustración 6 reporte de uso CPU por dispositivo durante el mes de julio 2022.

Se verifica que los dispositivos no cuentan con consumos críticos de CPU en promedio, sin embargo, los consumos máximos superan el 70% para el Host Name APPWEB01, se evidencias caídas fuertes de CPU a lo cual se recomienda validar con el administrador.

6.1 MEMORIA

A continuación, se observa el porcentaje de Memoria de los dispositivos:



Host Name	Host IP	AVG(Memory Util)	MAX(Memory Util)	MIN(Memory Util)
APPINT01	192.168.60.2	51.33%	72.43%	4.38%
APPWEB01	192.168.70.201	40.11%	81.02%	3.28%

Ilustración 7 reporte de uso memoria por dispositivo durante el mes de julio 2022

Se verifica que los dispositivos cuentan con un consumo promedio estable, pero se han presentado consumos críticos de un 81% para el APPWEB01.

7. EVENTOS RELEVANTES

A continuación, se observa el resumen de eventos relevantes de seguridad identificados por los dispositivos Perimetrales de seguridad.

7.0 Top de IPs con Malware

A continuación, se observa el top de IPs en los cuales se ha detectado malware por el dispositivo perimetral:

Destination IP	Event Name	COUNT
10.200.10.158	FortiGate ips malicious url	30
10.200.10.158	Gh0st.Rat.Botnet	14
10.200.10.158	Bladabindi.Botnet	13
10.200.10.157	FortiGate ips malicious url	5
10.200.10.157	Bladabindi.Botnet	4
10.200.10.158	Mirai.Botnet	3

192.168.70.32	Gh0st.Rat.Botnet	3
192.168.70.32	Bladabindi.Botnet	3
10.200.10.158	Mirai.Botnet	2
10.200.10.158	Bladabindi.Botnet	2
10.200.10.158	Bladabindi.Botnet	2
10.200.10.158	Mirai.Botnet	2
10.200.10.158	Mirai.Botnet	2
10.200.10.158	Mirai.Botnet	2
10.200.10.157	Gh0st.Rat.Botnet	2
192.168.70.32	Mirai.Botnet	2
10.200.10.158	Mirai.Botnet	2
10.200.10.158	Mirai.Botnet	2
10.200.10.158	Bladabindi.Botnet	2

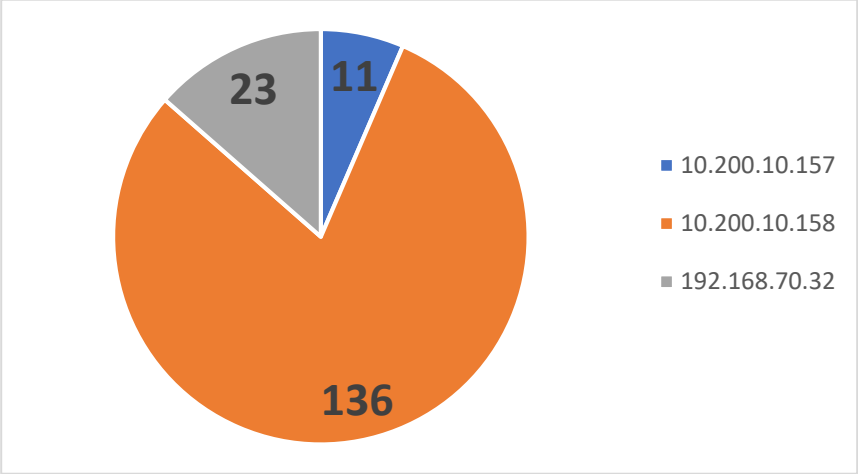


Ilustración 8 Top de IPs con malware reportados durante el mes de julio 2022

Se sugiere realizar una validación con el administrador de la red y los usuarios que hacen uso de los dispositivos en cual se detecta la IP 10.200.10.158 con varias firmas de Malware detectadas, mismo dispositivo que reflejo la mayor cantidad en el mes inmediatamente anterior, se recomienda inspeccionar los dispositivos 10.200.10.157 y 192.168.70.32 por la gran cantidad de detecciones.

7.1 Trafico de salida permitido por destino

En este gráfico se observa el top 10 de países a los cuales se realizan consultas de tráfico y que es permitido por los dispositivos perimetrales:

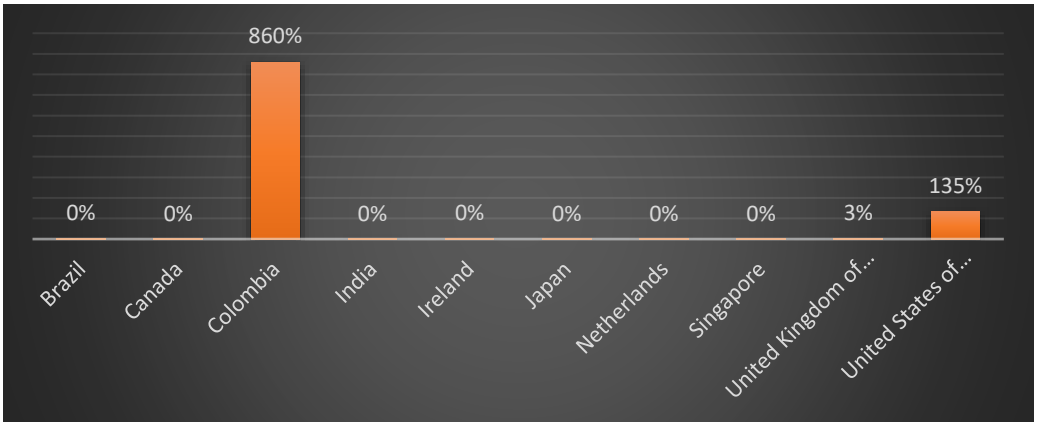


Ilustración 9 Top países de tráfico permitido durante el mes de julio 2022

Se observa que el top de países de destino que más consultan los usuarios de la compañía son Estados Unidos y Colombia con el 99%, se observa en el top de conexiones dominios sin riesgo, igual que el mes inmediatamente anterior.

7.2 Top de Fuentes con más conteos de Bloqueos

A continuación, se observa las fuentes que más tienen denegaciones realizadas por el dispositivo perimetral:

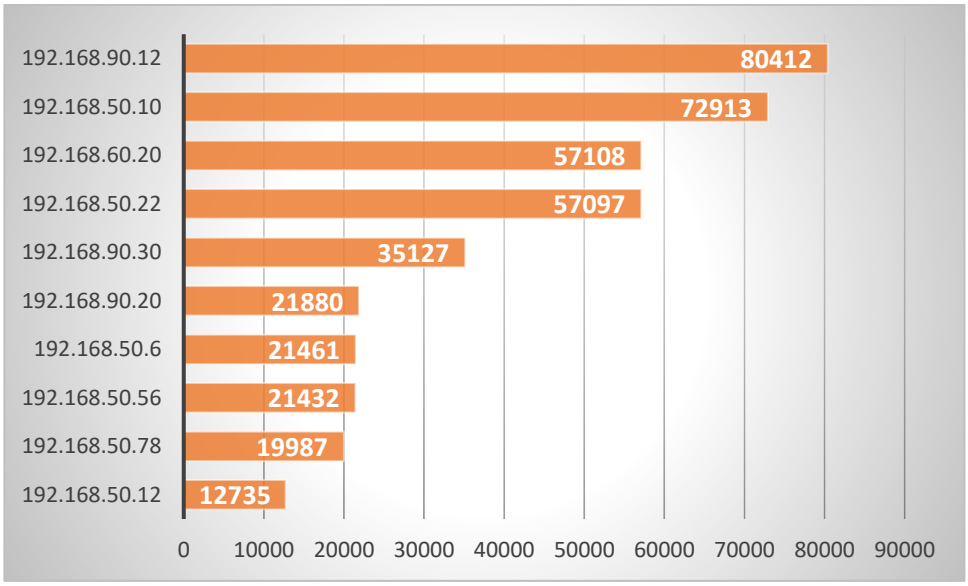


Ilustración 10 Top fuentes con más bloqueos reportados durante el mes de julio 2022

Se observa que en el TOP 10 de eventos se superan las 1000 interacciones, lo cual es un número elevado y continuo mes a mes, se recomienda su validación con el administrador.

7.3 Firewall Deny: Top de Destinos con más conteos de denegaciones

A continuación, se observa la cantidad de tráfico denegado por destino y detalle del top 10 de host de destino:

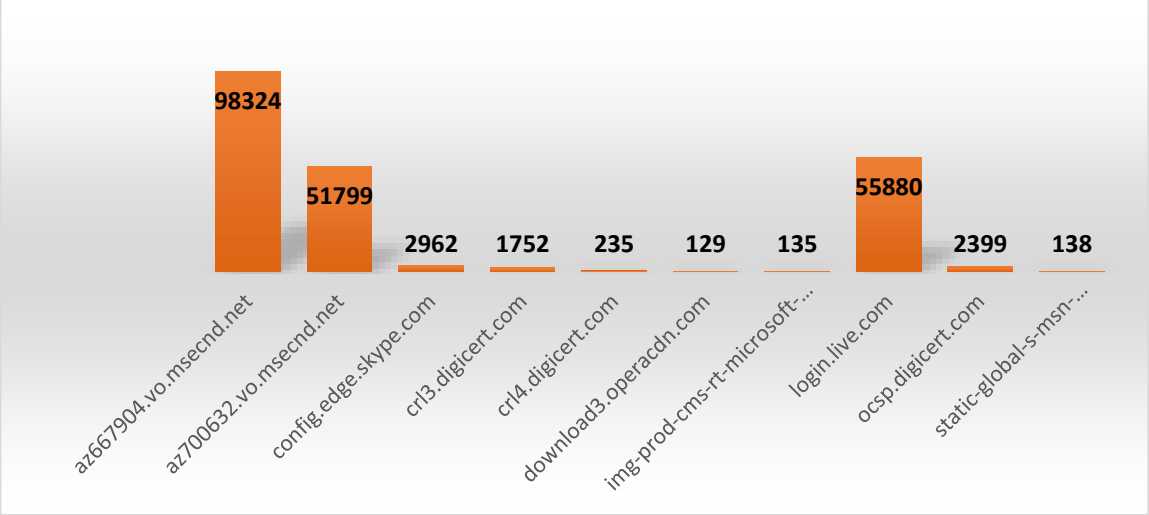


Ilustración 11 Top de categorías con más bloqueos reportados durante el mes de julio 2022

En la siguiente imagen podremos encontrar las categorías y páginas visitadas más relevantes, en donde observamos que el mayor destino fue az667904.vo.msecnd.net, seguido por az700632.vo.msecnd.net y login.live.com, las cuales son del servicio de blobs de Windows Azure y login de cuentas Microsoft respectivamente.

7.4 Firewall: Top de cambios realizados

A continuación, se observa la cantidad de cambios por tipo de cambio realizado y usuario.

Cuenta de Firewall Action	admin	No usuario	Total general
Add	100,00%	0,00%	100,00%
Edit	100,00%	0,00%	100,00%
update	0,00%	100,00%	100,00%
Total general	2,03%	97,97%	100,00%

Ilustración 12 Top de cambios reportados durante el mes de julio 2022

Se puede observar que el 98% de los cambios realizados son por actualización, seguido por el 2% de cambios realizados por el usuario admin.

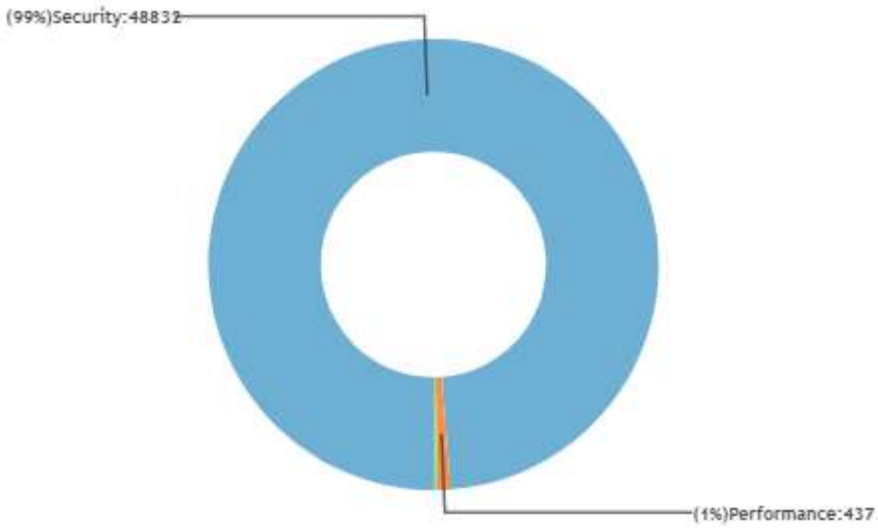
8. INCIDENTES

8.0 Vista Global

A continuación, se observa el total de los casos por categoría, teniendo en cuenta la siguiente nomenclatura de ID de incidencia que identifica la categoría de este:

1. Disponibilidad
2. Rendimiento
3. Seguridad

Se puede observar que la mayor parte de los incidentes con un total del 99% es asociada a la categoría de Security, seguido por la categoría de Performance con el 1% y la categoría de disponibilidad con el 0,1%.



Incident Category	Count
Security	48832
Performance	437
Availability	145

Ilustración 13 vista general de incidentes por categoría durante el mes de julio 2022.

8.1 Incidentes de Disponibilidad

El Top de incidentes reportado de disponibilidad con mayor criticidad y número de eventos que dispararon las reglas generadas durante el mes de julio 2022.

Event Name	Event Severity	Severity Category	Count
Missing specific performance metric from a device	10	HIGH	63
Server Down: No Ping Response	10	HIGH	29
WMI Service Unavailable	10	HIGH	22
SNMP Service Unavailable	10	HIGH	4
FortiSIEM Performance Monitoring Relay Not Working: All Devices delayed	10	HIGH	1
Service Down: No Response to STM: Has IP	9	HIGH	6
Server Degraded: Lossy Ping Response	8	MEDIUM	6
Service Degraded: Slow Response to STM: Has IP	7	MEDIUM	7
Sudden Decrease in Reported Events From A Host	7	MEDIUM	5
No performance metrics from a device	7	MEDIUM	2

Ilustración 14 Top incidentes de indisponibilidad durante el mes de julio 2022.

A continuación, se observa el top de dispositivos que más reportaron incidentes de disponibilidad:

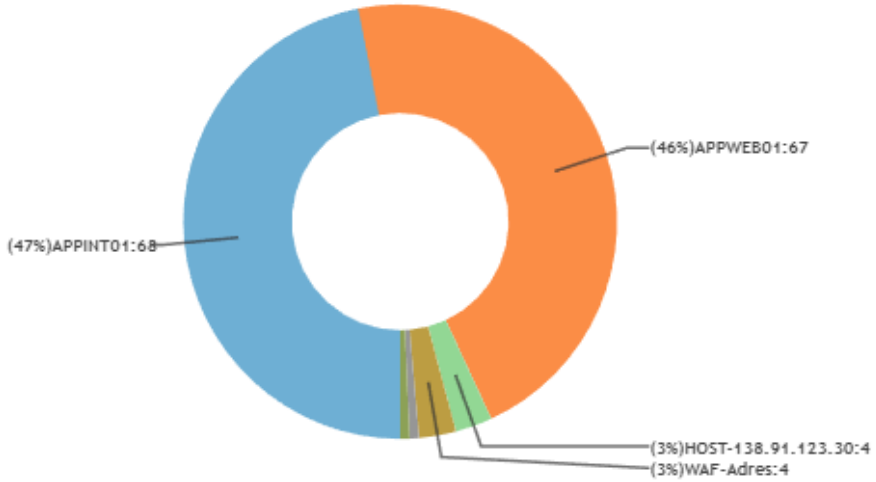


Ilustración 15 Top incidentes de indisponibilidad por dispositivo durante el mes de julio 2022.

Se puede observar que el dispositivo con mayor conteo de incidentes de disponibilidad es el dispositivo APPINT01 con 68 eventos, seguido del dispositivo APPWEB01 con 67 eventos.

A continuación, describiremos los eventos que más se generaron teniendo en cuenta el TOP de dispositivos y basándonos en su severidad ALTA para entender el porqué de dicho top y qué conclusiones se pueden tener sobre el análisis de la data.

Event Name	Event Severity	Severity Category	Count
Missing specific performance metric from a device	10	HIGH	63
Server Down: No Ping Response	10	HIGH	29
WMI Service Unavailable	10	HIGH	22
SNMP Service Unavailable	10	HIGH	4
FortiSIEM Performance Monitoring Relay Not Working: All Devices delayed	10	HIGH	1
Service Down: No Response to STM: Has IP	9	HIGH	6

- **Missing specific performance metric from a device**: Detecta que FortiSIEM no ha recibido una métrica de rendimiento específica de un dispositivo durante un período de tiempo estimado entre 120 y 600 segundos, lo cual puede deberse a una falla de conectividad entre los dispositivos, esto está alineado directamente con el evento Server Down: No Ping Response, con un promedio de 1 evento por día en un periodo de tiempo muy corto, esto aplica para los equipos APPWEB01 y APPINT01 ya que fueron los únicos que generaron dicho evento.
  Lo anterior se refleja también para el dispositivo APPWEB01 y APPINT01, así mismo hace referencia para **Server Down**: No Ping Response y la indisponibilidad de los protocolos SNMP y WMI, el cual puede deberse a una falla de conectividad, de acuerdo a la cantidad de eventos y SLA no representan un incidente.

8.2 Incidentes de rendimiento

El Top de incidentes de rendimiento por mayor criticidad y número de eventos que dispararon las reglas generadas durante el mes de julio 2022.

Event Name	Event Severity	Severity Category	Count
Server Disk Latency Warning	5	MEDIUM	302
Server Disk Latency Critical	9	HIGH	36
Server Disk Space Critical	9	HIGH	25
Sudden Increase in STM Response Times	7	MEDIUM	23
Sudden Increase in Network Interface Errors	7	MEDIUM	17
Server Disk space Warning	5	MEDIUM	17
Sudden Increase in WMI Response Times	7	MEDIUM	11
Sudden Increase in System Memory Usage	7	MEDIUM	4
Sudden Increase in Server Process Count	7	MEDIUM	1
Sudden Increase in SNMP Response Times	7	MEDIUM	1

Ilustración 16 Top incidentes de rendimiento durante el mes de julio 2022.

A continuación, se observa el top de dispositivos que más reportaron incidentes de rendimiento:

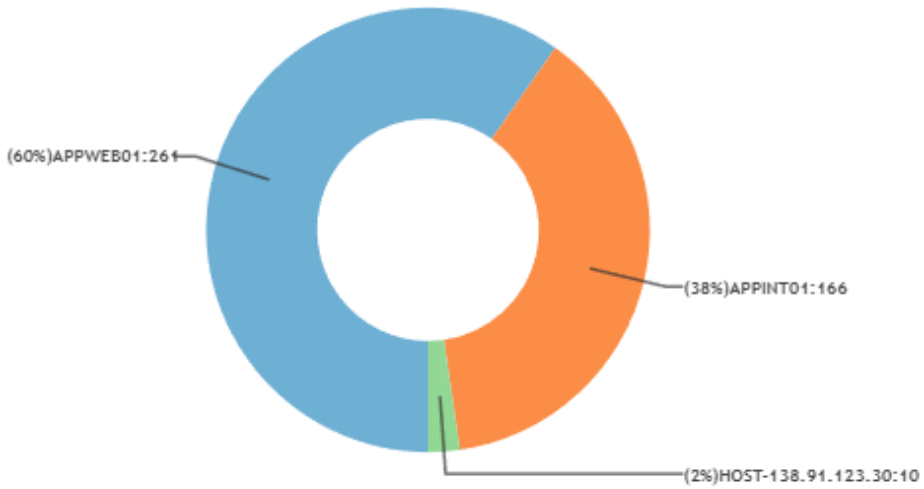


Ilustración 17 Top incidentes de rendimiento por dispositivo durante el mes de julio 2022.

Se puede observar que el dispositivo con mayor conteo de incidentes de rendimiento es el dispositivo APPWEB01 con 261 eventos, seguido del dispositivo APPINT01 con 166 eventos.

A continuación, describiremos los eventos que más se generaron teniendo en cuenta el TOP de dispositivos y basándonos en su severidad ALTA para entender el porqué de dicho top y qué conclusiones se pueden tener sobre el análisis de la data.

Host Name	Severity Category	Event Severity	Event Name	Count
APPINT01	HIGH	9	Server Disk Space Critical	20
APPINT01	HIGH	9	Server Disk Latency Critical	19
APPWEB01	HIGH	9	Server Disk Latency Critical	19
APPWEB01	HIGH	9	Server Disk Space Critical	5

La alerta de Latencia crítica para los dos equipos se refleja por que el servidor ha alcanzado un nivel crítico superior a 50ms en función de 2 lecturas sucesivas en un tiempo de 10 minutos, sin embargo el promedio de latencia para lectura esta en los 4ms y de 1ms para escritura.

Host Name	Disk Name	Host IP	Total Disk MB	AVG(Disk Capacity Util)	AVG(Free Disk MB)	COUNT(Matched Events)
APPINT01	L:\Log1	192.168.60.2	99.99 GB	100.00%	0 MB	9554
APPWEB01	L:\Log1	192.168.70.201	127.99 GB	88.29%	14.99 GB	9534
APPWEB01	F:\Reclamaciones	192.168.70.201	499.87 GB	85.09%	74.51 GB	9534
APPWEB01	G:\Data1	192.168.70.201	127.99 GB	84.55%	19.78 GB	9534

- **Server Disk Space Critical:** Se reporta por los discos L de APPINT01 y APPWEB01, el disco F y G de APPWEB01 los cuales superan el 80% de capacidad utilizada.

8.3 Incidentes de seguridad severidad alta

El Top 10 de incidentes de seguridad por mayor criticidad y número de eventos que dispararon las reglas generadas durante el mes de julio 2022.

Event Name	Event Severity	Severity Category	Count
Stealth Scan	9	HIGH	542
Sudden User Location Change	9	HIGH	6
Multiple Distinct IPS Events From Same Src	9	HIGH	5
DoS Attack detected by NIPS	9	HIGH	2
Large Outbound Transfer To Outside My Country	8	MEDIUM	32
Large Outbound Transfer	8	MEDIUM	21
Successful VPN Logon From Outside My Country	8	MEDIUM	20
Multiple Login Failures: Net Device: No Source IP	8	MEDIUM	1
Inappropriate Website access	7	MEDIUM	49159
System Exploit Detected by Network IPS	7	MEDIUM	167
Multiple IPS Detected Scans From Same Src	7	MEDIUM	63
Privilege Escalation Exploits	7	MEDIUM	10

Ilustración 18 Top incidentes de seguridad durante el mes de julio 2022.

A continuación, se observa el top de dispositivos que más reportaron incidentes de seguridad:

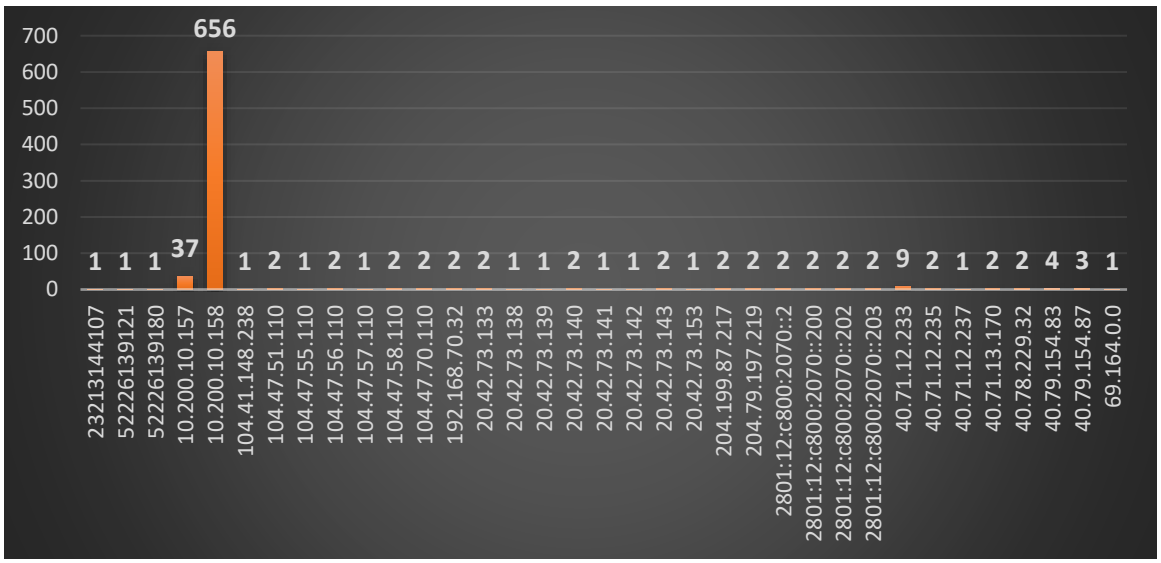


Ilustración 19 Top incidentes de seguridad por dispositivo durante el mes de julio 2022.

Se puede observar que el dispositivo con mayor conteo de incidentes de seguridad es el dispositivo con IP 10.200.10.158, con 656 eventos, es el mismo dispositivo que ha generado la mayor cantidad de registros por malware reportado en el mes inmediatamente anterior.

A continuación, describiremos los eventos que más se generaron teniendo en cuenta el TOP de dispositivos y basándonos en su severidad para entender el porqué de dicho top y qué conclusiones se pueden tener sobre el análisis de la data.

- **Stealth Scan**: Podemos validar que el target con mayor número de ataques es la ip 10.200.10.158, del total de los 656 ataques de los cuales se permitieron 38.

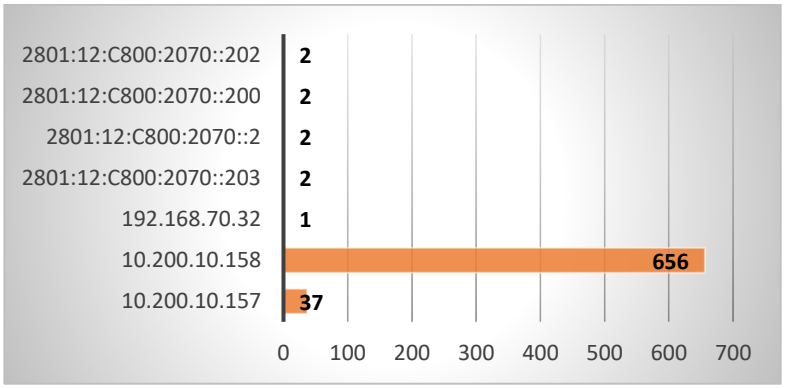


Ilustración 20 Top incidentes de Stealth Scan por dispositivo durante el mes de julio 2022.

Firmas	Acción del evento		
Etiquetas de fila	Deny	Permit	Total general
Cisco.Smart.Install.Feature.Enable.Scanner		7	7
Nmap.Script.Scanner	92		92
PHP.Diescan	1		1
ZGrab.Scanner	546	37	583
ZmEu.Vulnerability.Scanner	1		1
Muieblackcat.Scanner	1		1
Masscan.Scanner	17		17
Total general	**658**	**44**	**702**

Ilustración 21 Top incidentes de Stealth Scan por firmas durante el mes de julio 2022.

- **Sudden User Location Change:** Detecta cambio de ubicación para un usuario inviable en el periodo de tiempo. Esto puede indicar una credencial robada, validar con los siguientes usuarios si existe la aprobación de ingreso desde estás ubicaciones, así como el ingreso controlado.

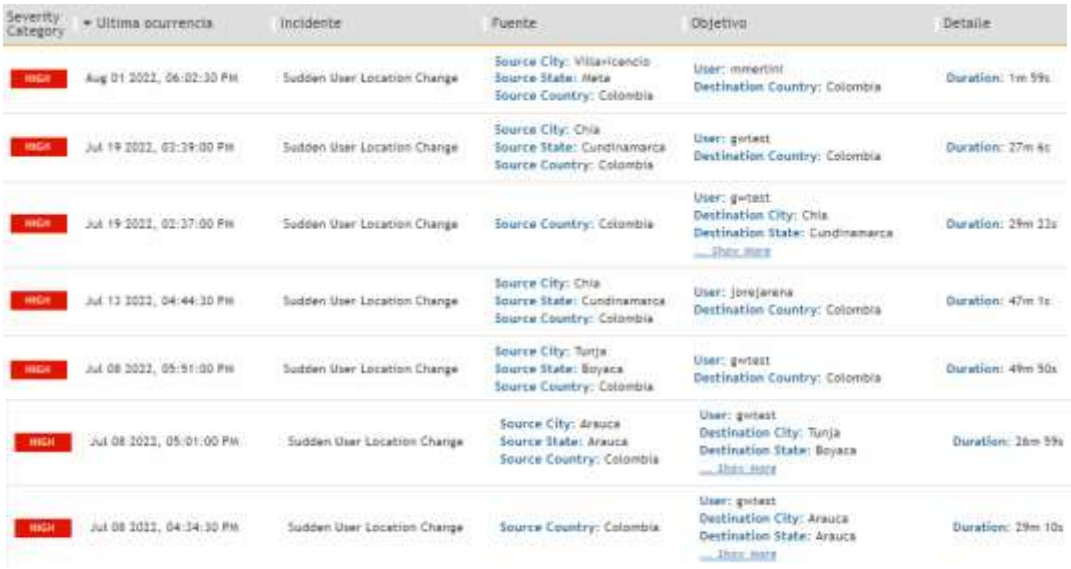


Ilustración 21 Top incidentes de Sudden User Location Change por firmas durante el mes de julio 2022.

- **Multiple Distinct IPS Events From Same Src**: Detecta múltiples eventos IPS desde la misma IP de origen en un corto período de tiempo, se evidencia que todos los eventos fueron denegados por el Firewall.

Etiquetas de fila	Deny	Total general
10.200.10.157	32	32
10.200.10.158	3732	3732
192.168.70.32	325	325
2801:12:c800:2070::2	2	2
2801:12:c800:2070::200	2	2
2801:12:c800:2070::202	2	2
2801:12:c800:2070::203	6	6
Total general	**4101**	**4101**

A continuación las firmas de eventos IPS que más se reportaron:

FortiGate-ips-signature-50825	162
FortiGate-ips-signature-50899	188
Generic.XXE.Detection	158
Mirai.Botnet	88
MobileIron.MDM.Unauthenticated.Remote.Code.Execution	68
Nmap.Script.Scanner	149
PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	355
ThinkPHP.Controller.Parameter.Remote.Code.Execution	167
TrueOnline.ZyXEL.P660HN.V1.Unauthenticated.Command.Injection	1584
ZGrab.Scanner	641

Ilustración 22 Top incidentes de Multiple Distinct IPS Events From Same Src durante el mes de julio 2022.

- **DoS Attack detected by NIPS**: Detecta ataques de denegación de servicio de alta gravedad en un servidor que normalmente explota una vulnerabilidad de código y provoca una utilización excesiva de recursos (CPU o memoria) en el servidor, en la imagen siguiente se evidencian los dos eventos presentados los cuales fueron denegados.

Event Action	Event Name	Attack Name	Destination IP	Source IP	COUNT(Matched Events)
1 (Deny)	Linux.Kernel.TCP.SACK.Panic.DoS	Linux.Kernel.TCP.SACK.Panic.DoS	10.200.10.158	131.159.24.205	11
1 (Deny)	Linux.Kernel.TCP.SACK.Panic.DoS	Linux.Kernel.TCP.SACK.Panic.DoS	192.168.70.32	131.159.24.205	2

Ilustración 23 Top incidentes de DoS Attack detected by NIPS durante el mes de julio 2022.

- **Successful VPN Logon From Outside My Country:** Se detectan los siguientes usuarios, los cuales se han conectado desde las diferentes ciudades, lo cual también aplica en gran parte para la transferencia.

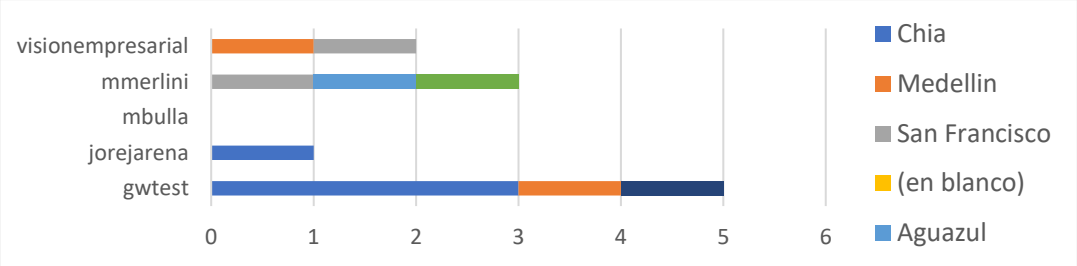


Ilustración 24 Top incidentes de Successful VPN Logon From Outside My Country durante el mes de julio 2022.

- **System Exploit Detected by Network IPS**: A continuación el Top 10 múltiples eventos IPS los cuales realizan un intento de ataque para explotar una vulnerabilidad de ejecución remota de código, todos los eventos fueron denegados por el Firewall, nuevamente la IP 10.200.10.158 es el destino de la mayor cantidad de eventos, adicional el TOP de los 10 países desde los cuales se han generado la mayor cantidad de eventos IPS.

Etiquetas de fila	Cuenta
Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	29
Dasan.GPON.Remote.Code.Execution	34
D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	27
D-Link.DSL-2750B.CLI.OS.Command.Injection	17
MS.Windows.HTTP.sys.Request.Handling.Remote.Code.Execution	12
NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	39
PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	30
Shenzhen.TVT.DVR.Remote.Code.Execution	8
ThinkPHP.Controller.Parameter.Remote.Code.Execution	8
TrueOnline.ZyXEL.P660HN.V1.Unauthenticated.Command.Injection	700
Total general	904

Source Country	Cuenta
China	209
Hong Kong	63
Korea (the Republic of)	37
Mexico	83
Russian Federation	40
Sweden	32
Taiwan	40
Turkey	38
Ukraine	34
United States of America	136
Total general	**712**

Ilustración 24 Top incidentes de países que han generado mayor cantidad de eventos durante el mes de julio 2022.

- Se adjunta informe con las URL reportadas para Inapropiate Web Site.

9. ACTIVIDADES ADICIONALES RELEVANTES DEL MES

Para el mes de julio no se presentaron actividades relevantes.

10. ACCIONES DE MEJORA

Instalación de agentes para los servidores Windows y Linux. Los agentes proporcionan una forma limpia y eficiente de recopilar exactamente los datos que se necesitan. Los agentes de FortiSIEM son muy livianos y no consumen más del 5 % de la CPU y la memoria del sistema. Los agentes de FortiSIEM tienen la siguiente funcionalidad:

- Recopile cualquier registro de eventos de Windows, incluidos los registros de eventos de seguridad, aplicación y rendimiento, registros de DHCP/DNS, registros de Sysmon, etc.
- Recopilar archivos de registro personalizados
- Detectar cambios en el registro
- Detectar lectura, escritura y edición de archivos (FIM) con contexto de usuario agregado

- Ejecute cualquier comando de PowerShell y envíe el resultado como registros; esto permite a los usuarios capturar datos a intervalos periódicos y enviarlos a FortiSIEM.
- Detectar la inserción, eliminación, lectura y escritura de medios extraíbles

Configuración de los protocolos SNMV3 en el dispositivo AdresFSCo, FortiGate-600E y WAF-Adres, para recopilar información complementaría como: Tiempo de actividad, CPU/memoria/interfaz de red/utilización de espacio en disco, utilización de espacio de intercambio, errores de interfaz de red, recuento de procesos en ejecución, cambio de software instalado, utilización de CPU/memoria en proceso en ejecución, inicio/detención de proceso en ejecución, activación/desactivación de puerto TCP/UDP.

11. CONCLUSIONES

1. Se recomienda realizar ajuste de políticas para el bloqueo de las firmas indicadas en la presentación, ya que la acción de la regla fue **permitida,** incluir la firma Cisco.Smart.Install.Feature.Enable.Scanner, ya que los 7 eventos fueron permitidos.

2. Se sugiere validar con el administrador de la red el equipo con IP 10.200.10.158, ya que es el que genera mayor reporte de eventos, este es el que ha generado la mayor cantidad de eventos todos los meses.

3. Validar las IPs 192.168.90.12 y 192.168.50.10, que han generado más bloqueos por denegación de fuentes.

4. Validar los discos L de APPINT01 y el disco G de APPWEB01 los cuales superan el 80% de capacidad utilizada que a su vez genera reportes de latencia.

5. Validar las conexiones VPN desde fuera de la ciudad si son autorizadas recomendados en el mes pasado.