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	1/11/2020	**Fecha de Terminación**	30/11/2022

Periodo del Informe de Actividades	**Desde**	1/10/2022	**Hasta**	31/10/2022
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 Adición No. 3 por la suma de $ 159.618.059 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: 25/11/2022

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	$3.057.756.899,48	$ 2.431.051.557,78	$313.299.999,87	$0	$313.405.341,83

La ADRES cancelará al CONTRATISTA, la suma de trescientos trece millones doscientos noventa y nueve mil novecientos noventa y nueve con ochenta y siete centavos ($313.299.999,87)

PAGO DE SEGURIDAD SOCIAL PERSONAS NATURALES
Mes de ejecución contractual

CONCEPTO	PLANILLA No.	VALOR	PERIODO		FECHA DE PAGO
			DESDE	HASTA	
Salud	1049960060	$82.982.200	1/11/2022	30/11/2022	4/11/2022
Pensión			1/10/2022	31/10/2022	4/11/2022
ARL			1/10/2022	31/10/2022	4/11/2022

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-168 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., 29/11/2022

[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-168

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	17/11/2022, 16:33
Expedición	17/11/2022, 16:33
Vencimiento	17/12/2022

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: 3 (Línea No.2)	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	51,029,323.60	0 %	49,243,297.27
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	26,996,082.40	0 %	26,051,219.52
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 %	2,559,205.83
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	npn03--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 %	2,447,879.86
25	npn03--Servicios Complementarios - Experto Master - Región 1 - Hora/M- Cantidad: 20 (Línea No. 27)	1.00	226,066.90	0 %	218,154.56
26	npn03--Servicios Complementarios - Experto Master en Base de Datos MSSQLServer - Región 1 - Hora/M- Cantidad: 20 (Línea No. 28)	1.00	226,066.90	0 %	218,154.56
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--IaaS Seguridad - Firewall Nueva Generación - Media baja Capacidad - Oro - Hosting físico - Rol de Firewall - 15 Gbps - Sesiones Concurrentes - 7000000 - Mes - Cantidad: 2 (Línea No. 30)	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 items: 32

Valor en Letras:
Doscientos noventa y ocho millones setecientos setenta y ocho mil quinientos cinco pesos m/cte con sesenta y uno cent.

Condiciones de Pago:
Crédito - Cuota No. 001 vence el 2022-12-17 por $ 298,778,505.61

Observaciones:
Observaciones:
Nota: Periodo Servicio Octubre 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

Total Bruto	308,273,264.76
IVA 19%	5,026,735.11
Retefuente 3.5%	10,789,564.25
ReteIVA 15%	754,010.27
ReteICA 9.66	2,977,919.74
Total a Pagar	**298,778,505.61**

Por favor tener en cuenta el siguiente porcentaje de participación de los miembros de la UT en el presente documento:
1. Internexa SA 8,79%
2 Infraestructura Virtual SAS 91,21%
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 - 91.21%
Internexa SA - NIT 811.021.654 - 8.79%

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: dc824882479b61c1a23d53a3aed697f7d40fa96b4f0d9033a7e1c64bb547dd3254efb8633077360e469a2b7dc56bb41e

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	2022-11-04, 09:59:15 AM
Periodo de Cotización Otros Riesgos	octubre de 2022
Periodo de Cotización Para Salud	noviembre de 2022
Empresa	INFRAESTRUCTURA VIRTUAL SAS
NIT	NI 900486933
Código Sucursal (Nombre)	( )
Referencia de Pago/ Número Planilla	1049960060
Tipo de Planilla	E
Número Transacción Bancaria/ CUS	1740559672
Banco	(1001) - BANCO DE BOGOTA
Valor	$ 82.982.200
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	17	$ 11.400.900	$ 0
N800229739	230201	PROTECCION FONDO DE PENSIONES OBLIGATORIAS	5	$ 9.989.800	$ 0
N900336004	25-14	COLPENSIONES	7	$ 7.420.800	$ 0
N800227940	231001	COLFONDOS	12	$ 9.785.200	$ 0
N800253055	230901	OLD MUTUAL SKANDIA	3	$ 5.370.800	$ 0
N900156264	EPS037	NUEVA EPS S.A.	1	$ 80.000	$ 0
N800251440	EPS005	ENTIDAD PROMOTORA DE SALUD SANITAS S.A.	13	$ 8.049.500	$ 0
N830003564	EPS017	ENTIDAD PROMOTORA DE SALUD FAMISANAR LIMITADA CAFAM-COLSUBSIDIO	9	$ 2.799.100	$ 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	$ 69.100	$ 0
N830113831	EPS001	ALIANSALUD EPS S.A.	2	$ 3.440.000	$ 0
N800130907	EPS002	SALUD TOTAL S.A. ENTIDAD PROMOTORA DE SALUD	2	$ 340.000	$ 0
N800088702	EPS010	EPS SURA	9	$ 2.881.100	$ 0
N860066942	EPS008	COMPENSAR ENTIDAD PROMOTORA DE SALUD	5	$ 2.277.300	$ 0
N901037916	MIN002	ADMINISTRADORA DE LOS RECURSOS SS ADRES	1	$ 2.162.800	$ 0
N800226175	14-25	RIESGOS PROFESIONALES COLMENA S.A COMPANIA DE SEGUROS DE VIDA	45	$ 2.211.900	$ 0
N890500675	CCF36	CAJA DE COMPENSACION FAMILIAR DEL ORIENTE COLOMBIANO COMFAORIENTE	1	$ 168.000	$ 0
N860066942	CCF24	CAJA DE COMPENSACION FAMILIAR COMPENSAR	38	$ 8.184.400	$ 0
N890303208	CCF57	COMFANDI	5	$ 833.100	$ 0
N899999034	PASENA	SENA	11	$ 2.189.800	$ 0
N899999239	PAICBF	INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR	11	$ 3.284.600	$ 0
		SubTotales:		$ 82.982.200	$ 0
		Total a Pagar:			$ 82.982.200

compensar | miplanilla.com

REPORTE RESUMEN DE PAGO

Información básica de la planilla

Empresa:	INTERNEXA S.A.	**NIT:**	811021654
Tipo Planilla:	E	**Periodo liquidación Pensiones:**	octubre 2022
Sucursal o Dependencia:	PRINCIPAL	**Periodo liquidación Salud:**	noviembre 2022
Número de Radicación:	62754818	**Total a pagar:**	$769,849,300
Fecha de vencimiento:	28/10/2022	**Total de empleados:**	231
Fecha de Pago:	26/10/2022	**Número de Administradoras:**	25

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:**	1724167702
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	231		$0	$29,933,200
230201	800229739	Proteccion (ING + Proteccion)	99		$0	$148,997,900
230301	800224808	Porvenir	28		$0	$42,042,400
230901	800253055	FONDO DE PENSIONES OBLIGATORIAS SKANDIA	10		$0	$16,814,500
231001	800227940	Colfondos	14		$0	$19,838,600
25-14	900336004	Administradora Colombiana de Pensiones -	71		$0	$126,042,300
CCF04	890900841	Comfama Caja de Compensacion Fliar	163		$0	$59,217,300
CCF07	890101994	Comfamiliar del Atlantico Caja de Compensacion	2		$0	$1,299,400
CCF11	890806490	Caja de Compensacion Familiar de Caldas	1		$0	$93,400
CCF24	860066942	Compensar Caja de Compensacion Fliar	53		$0	$21,304,700
CCF37	890500516	Comfanorte Caja de Compensacion Fliar	1		$0	$93,400
CCF40	890201578	Comfenalco Santander Caja de Compensacion	1		$0	$831,600
CCF57	890303208	Comfamiliar Andi Comfandi Caja de	2		$0	$1,442,300
EPS001	830113831	ALIANSALUD EPS S.A.	5		$0	$4,859,000
EPS002	800130907	Salud Total EPS	6		$0	$9,109,600
EPS005	800251440	Sanitas EPS	37		$0	$41,541,500
EPS008	860066942	Compensar EPS	15		$0	$16,141,100

Código	NIT	Administradoras	Num. Afiliados	*Número de incapacidad por riesgos laborales	Valor descontado en incapacidad y/o licencia	Total Pagado
EPS010	800088702	EPS Sura	157		$0	$143,420,200
EPS017	830003564	Famisanar EPS Cafam Colsubsidio	3		$0	$1,629,400
EPS018	805001157	Servicio Occidental de Salud S.A. S.O.S EPS	1		$0	$192,000
EPS037	900156264	Nueva Promotora de Salud - Nueva EPS	6		$0	$2,101,900
ESSC24	900226715	EPS-S Coosalud	1		$0	$93,400
ESSC62	900935126	ASMET SALUD EPS SAS	1		$0	$125,000
PAICBF	899999239	ICBF Instituto Colombiano de Bienestar Familiar	135		$0	$49,610,000
PASENA	899999034	SENA	135		$0	$33,075,200
						$769,849,300

***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 nueve (09) días del mes de noviembre 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-3042-22

Señores
Internexa S.A.
Medellín

Certificación de parafiscales

Fui nombrado Revisor Fiscal de INTERNEXA S.A., identificada con NIT 811.021.654-9 el 22 de marzo de 2022. Desde mi nombramiento he desarrollado los procedimientos necesarios para cumplir con mis funciones como Revisor Fiscal.

Los registros contables por el periodo comprendido del 1 de mayo al 31 de octubre 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", 2401010100- "Prove Nles Bnes/Serv" y las planillas de autoliquidación de aportes, incluyen el pago de aportes a las entidades respectivas, como se detalla a continuación:

Mes de causación	Número de planilla Integrada de Liquidación de Aporte (PILA)	Valor Pagado	Mes de pago	Estado de la planilla
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
Agosto 2022	61342137	722,479,000	Agosto 2022	Pagado
Septiembre 2022	62030378	710,365,300	Septiembre 2022	Pagado
Octubre 2022	62754818	769,849,300	Noviembre 2022	Pagado

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

De acuerdo con la Resolución Nº 006720 de 2021 emitida por el Servicio Nacional de Aprendizaje-SENA, la compañía INTERNEXA S.A. debe cumplir con una cuota obligatoria de 9 aprendices Sena.

De acuerdo con el maestro de empleados de INTERNEXA S.A. al 31 de octubre del 2022 la compañía cumplió con la cuota obligatoria de aprendices, dando cumplimiento a lo establecido en la Resolución Nº 006720 del 12 de agosto de 2021.

Building a better working world

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,

Esta certificación 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: 2022.11.03 09:26:16 -05'00'

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

Medellín, Antioquia
3 de noviembre de 2022

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 octubre– 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		Enlanube
Servicio entregado		Nube Privada
Modelo de servicio		**PaaS**
Fecha		10 de noviembre 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**.

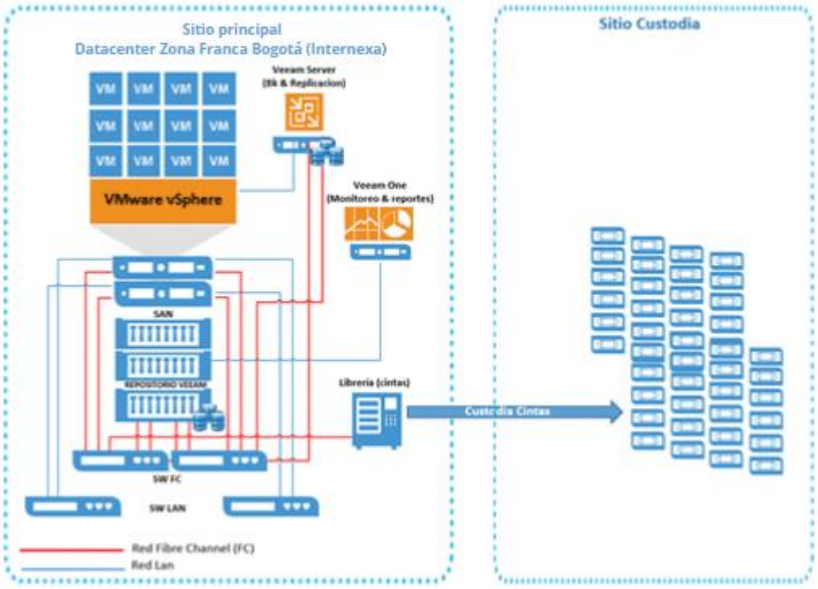


Figura 1. Infraestructura de la solución.

A continuación, se encuentra la topología actual.

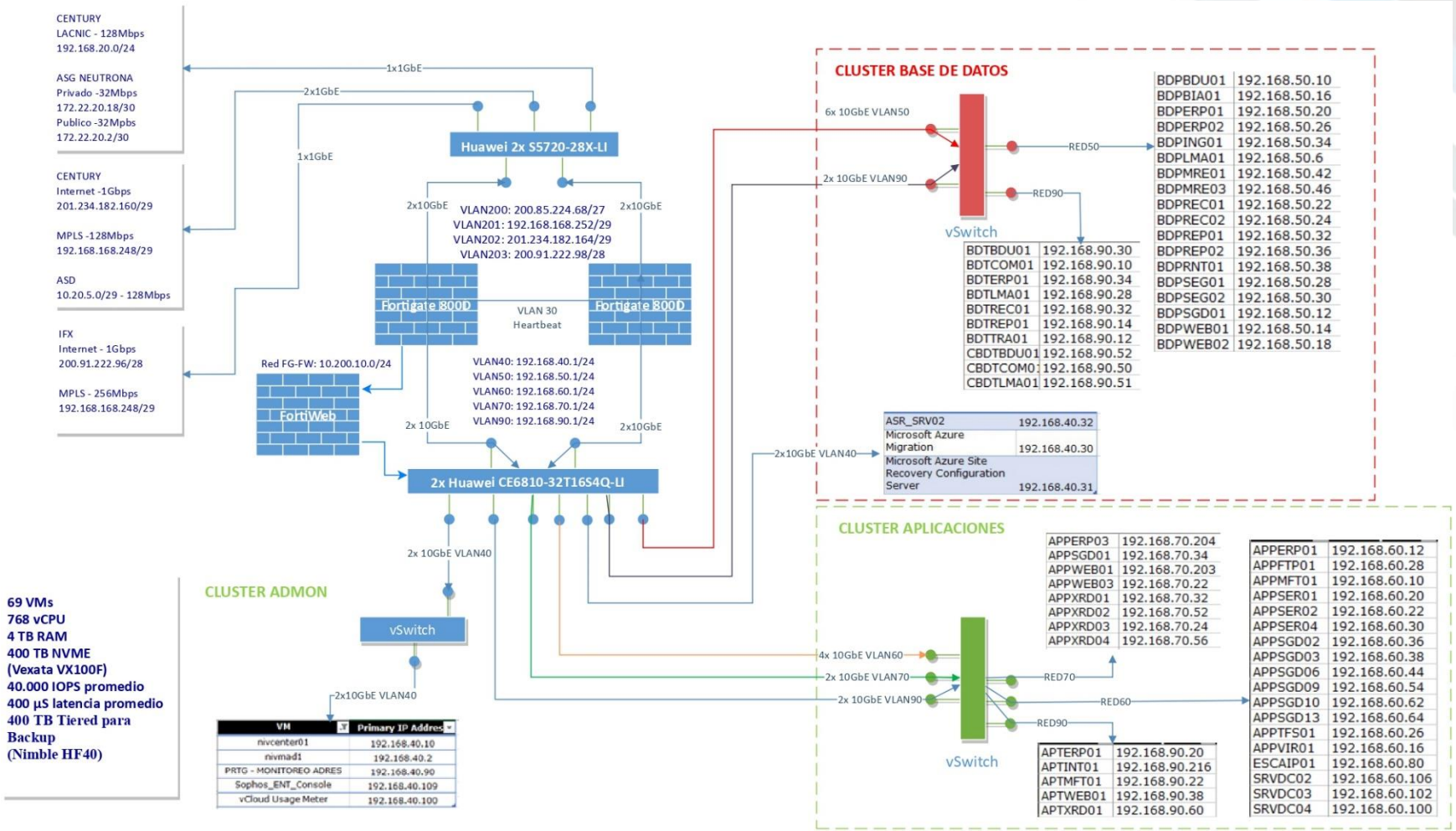


Figura 2. Topología actual

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	1.655
17	BDPSEG01	Microsoft Windows Server 2012 R2	16	32	2	5	828
18	BDPSEG02	Microsoft Windows Server 2012 R2	16	32	2	5	794
19	BDPWEB01	Microsoft Windows Server 2012 R2	32	98	2	13	11.219
20	BDPWEB02	Microsoft Windows Server 2016	16	81	1	13	5.760
21	BDPRNT01	Microsoft Windows Server 2019	16	81	1	13	11.084
22	BDTBDU01	Microsoft Windows Server 2019	16	65	1	7	7.404
23	BDTCOM01	Microsoft Windows Server 2019	20	98	1	16	30.015
24	BDTERP01	Microsoft Windows Server 2012 R2	16	32	2	7	7.282
25	BDTLMA01	Microsoft Windows Server 2019	16	65	1	10	14.154
26	BDTREC01-26112021	Microsoft Windows Server 2019	16	65	2	5	8700
27	BDTREP01	Microsoft Windows Server 2016	16	32	1	6	934
28	BDTTRA01	Microsoft Windows Server 2019	16	65	1	11	14.131
29	ASR_SRV02	Microsoft Windows Server 2016	16	32	1	2	1.204
30	ESCAIP01	Microsoft Windows Server 2019	16	32	2	1	155
31	BDPREP03	Microsoft Windows Server 2019	16	32	1	2	1.277
32	UBDPREC02	Microsoft Windows Server 2019	32	131	1	7	4.358
33	UBDPSEG01	Microsoft Windows Server 2019	16	32	1	5	860
34	UBDPSEG02	Microsoft Windows Server 2019	16	32	1	5	860
35	UBDTREC01	Microsoft Windows Server 2019	16	65	1	5	8649
36	UBDTREP01	Microsoft Windows Server 2019	16	32	1	6	934
37	BDDFAB01	Microsoft Windows Server 2019	32	131	1	6	3864
			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	925
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	1.544
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	512
9	APPSER01	Microsoft Windows Server 2019	16	32	2	6	607
10	APPSER02	Microsoft Windows Server 2019	16	32	1	24	63.395
11	APPSER04	Microsoft Windows Server 2019	16	32	2	10	12.992
12	APPSGD01	Microsoft Windows Server 2019	16	65	2	6	828
13	APPSGD02	Microsoft Windows Server 2019	16	65	2	6	2270
14	APPSGD07	Microsoft Windows Server 2019	16	32	2	5	673
15	APPRECDT01	Microsoft Windows Server 2019	16	32	2	3	2.425
16	APPSGD09	Microsoft Windows Server 2019	16	32	2	14	29.154
17	APPSGD10	Microsoft Windows Server 2019	16	65	2	12	37.605
18	APPSGD13	Microsoft Windows Server 2019	16	32	2	5	8.844
19	APPTFS01	Microsoft Windows Server 2019	16	32	2	6	1000
20	APPVIR01	Microsoft Windows Server 2019	16	32	1	12	24.913
21	APPWEB01	Microsoft Windows Server 2019	16	65	2	8	2.104
22	APPWEB02	Microsoft Windows Server 2019	16	65	2	6	951
23	APPWEB03	Microsoft Windows Server 2019	16	32	2	6	540
24	APPWEB_07	Microsoft Windows Server 2019	16	32	2	6	689
25	APTERP01	Microsoft Windows Server 2012 R2	16	32	2	6	1.045
26	APTINT01	Microsoft Windows Server 2019	16	32	2	6	737
27	APTMFT01	Microsoft Windows Server 2019	16	32	2	8	2.692

28	APTWEB01	Microsoft Windows Server 2019	16	32	1	6	923
29	APPXRD01	Ubuntu Linux	6	32	2	1	544
30	APPXRD02	Ubuntu Linux	6	32	2	1	544
31	APPXRD03N	Ubuntu Linux	16	32	1	1	544
32	APPXRD04	Ubuntu Linux	16	32	2	1	557
33	APTXRD01	Ubuntu Linux	16	32	2	1	557
34	APDFAB01	Microsoft Windows Server 2022	16	32	1	3	426
35	APPLOG01	Ubuntu Linux	16	32	1	1	163
36	APTERP02	Microsoft Windows Server 2016	16	32	1	3	852
37	APPSGD06	Microsoft Windows Server 2019	16	32	2	5	673
			548	1409			

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.

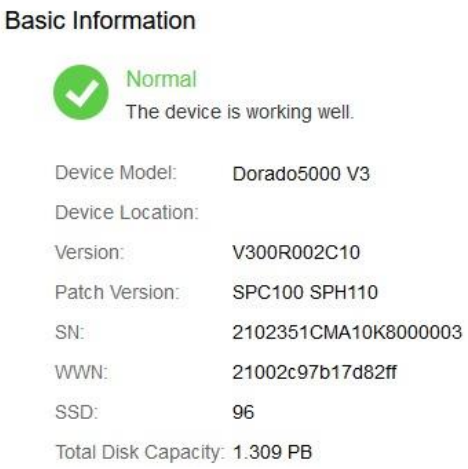


Figura 3. Información de identificación del Almacenamiento aprovisionado.

Dentro del almacenamiento Huawei actualmente a nivel de producción se están consumiendo 620 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	427.605
APPMFT01_0001	VMFS	1	7.295.584
APPMFT01_0002	VMFS	1	6.249.528
APPMFT01_0003	VMFS	1	12.585.168
APPSER01_0001	VMFS	2	2.705.738
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	9.668.234
APPSER02_0005	VMFS	1	7.342.280
APPSER04_0001	VMFS	2	15.098.609
APPSGD09_0001	VMFS	1	12.616.952
APPSGD09_0002	VMFS	1	11.608.167
APPSGD09_0003	VMFS	1	4.932.678
APPSGD10_0001	VMFS	1	7.722.259
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	2.426.178
APPVIR01_0001	VMFS	1	8.389.696
APPVIR01_0002	VMFS	1	8.389.688
APPVIR01_0003	VMFS	1	8.138.269
ASR_0001	VMFS	3	4.135.686
BDDFAB01_0001	VMFS	1	3.871.209
BDPBIA01N_0001	VMFS	1	952.967
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	132.414
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	2.098.153
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	2.098.152
BDPCOM01N_0011	VMFS	1	2.098.150
BDPCOM01N_0012	VMFS	1	2.098.151
BDPCOM01N_0013	VMFS	1	2.098.157
BDPCOM01N_0014	VMFS	1	3.115.003
BDPCOM01N_0015	VMFS	1	4.195.311
BDPCOM01N_0016	VMFS	1	3.138.826
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	329.490
BDPERP01N_0002	VMFS	1	296.365
BDPERP01N_0003	VMFS	1	68.012
BDPERP01N_0004	VMFS	1	1.050.058
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	3.245.889
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	11.004.316
BDPMRE01_0002	VMFS	1	12.583.996
BDPMRE02_0001	VMFS	1	11.284.123
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	2.501.315
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	2	1.721.676
BDPREC01N_0001	VMFS	1	1.738.469
BDPREC01N_0002	VMFS	1	2.098.971
BDPREC01N_0003	VMFS	1	2.098.759
BDPREC01N_0004	VMFS	1	2.098.651
BDPREC01N_0005	VMFS	1	2.098.674
BDPREC01N_0006	VMFS	1	1.050.058
BDPREC02N_0001	VMFS	1	689.776
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	0	1.510
BDPSGD01_0002	VMFS	0	1.490
BDPSGD01_0003	VMFS	0	1.510
BDPSGD01_0004	VMFS	0	1.490
BDPWEB01_0001	VMFS	1	11.221.183
BDPWEB02_0001	VMFS	2	16.845.914
BDTERP01_0001	VMFS	1	7.246.604
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	14.133.888
CBDTBDU01_0001	VMFS	1	7.406.965
CBDTCOM01_0001	VMFS	1	657.065
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	8.914.284
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	26	35.064.193
DS_APPS_0002	VMFS	5	13.031.764
DS_BD_0001	VMFS	12	7.579.482
DS_BD_0003	VMFS	2	5.571.695
DS_BD_0004	VMFS	1	8.701.123
DS_HUAWEI_ADMON	VMFS	12	4.057.181
UBDPBDU01_0001	VMFS	1	1.908.488
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	1.049.832
UBDPBDU02_0001	VMFS	1	1.908.442
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	1.050.058
UBDPBDU02_0011	VMFS	1	1.050.058
UBDPBDU02_0012	VMFS	1	1.050.058
UBDPLMA01_0001	VMFS	1	832.233
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	2.098.662
UBDPLMA01_0011	VMFS	1	2.098.651
UBDPLMA02_0001	VMFS	1	832.219
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	2.098.651
UBDPLMA02_0011	VMFS	1	2.098.651
VeeamBackup_VeeamADRES	NFS	0	848.861
			620.439.676

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.

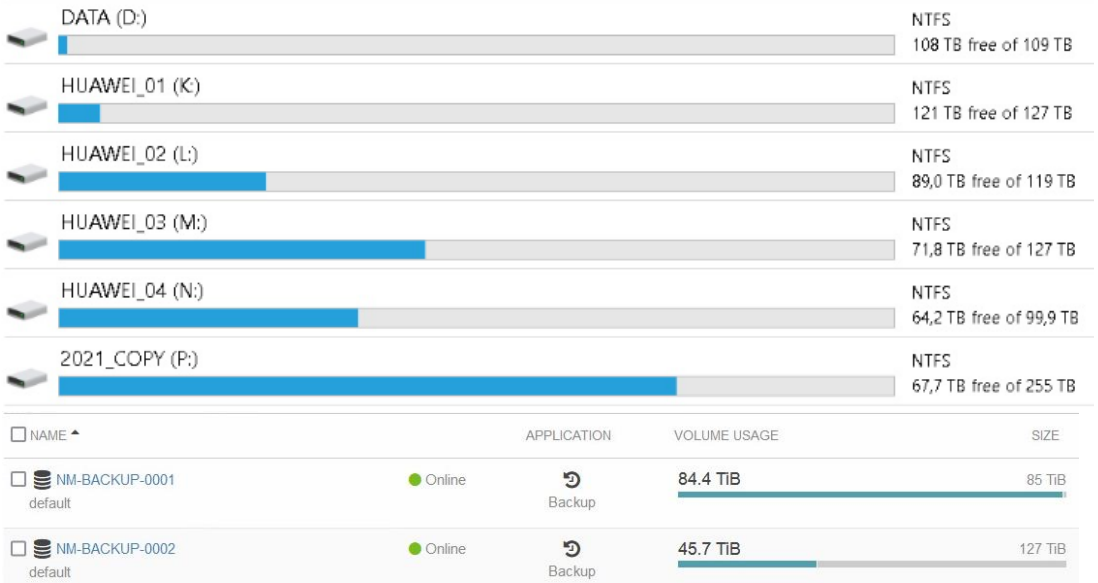
3. DISPONIBILIDAD DEL SERVICIO

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 445,3 TB), políticas diarias y semanales.

Figura 5. Consumo de back up Repositorios Veeam



Repositorio	Tamaño uso [TB]
DATA	1
HUAWEI_01	6
HUAWEI_02	30
HUAWEI_03	55,2
HUAWEI_04	35,7

2021_COPY	187,3
NIMBLE_01	84,4
NIMBLE_02	45,7
TOTAL	**445,3**

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 octubre 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 octubre 2022.

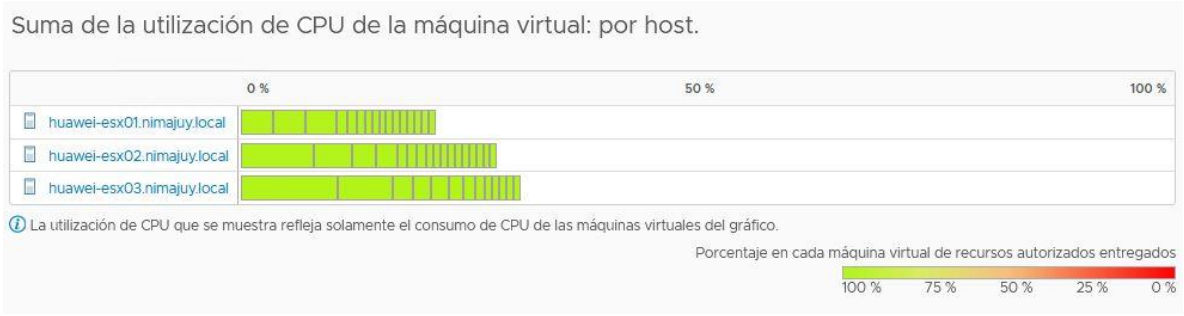


Figura 6. Consumo de CPU en Cluster de Aplicaciones

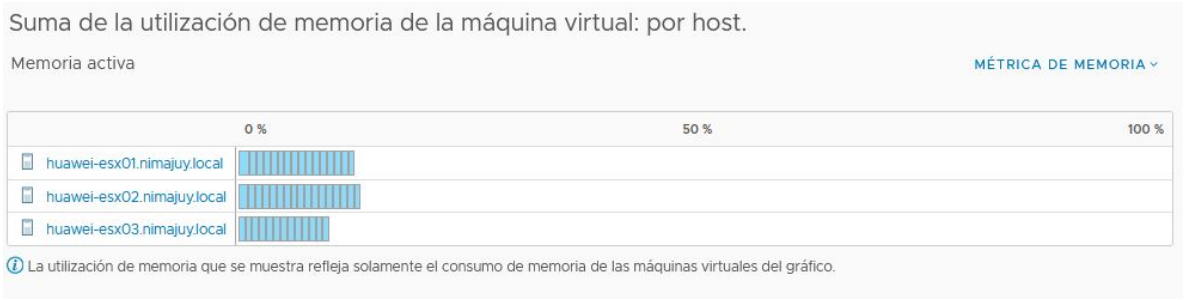


Figura 7. Consumo de memoria en Cluster de Aplicaciones.

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 octubre 2022.

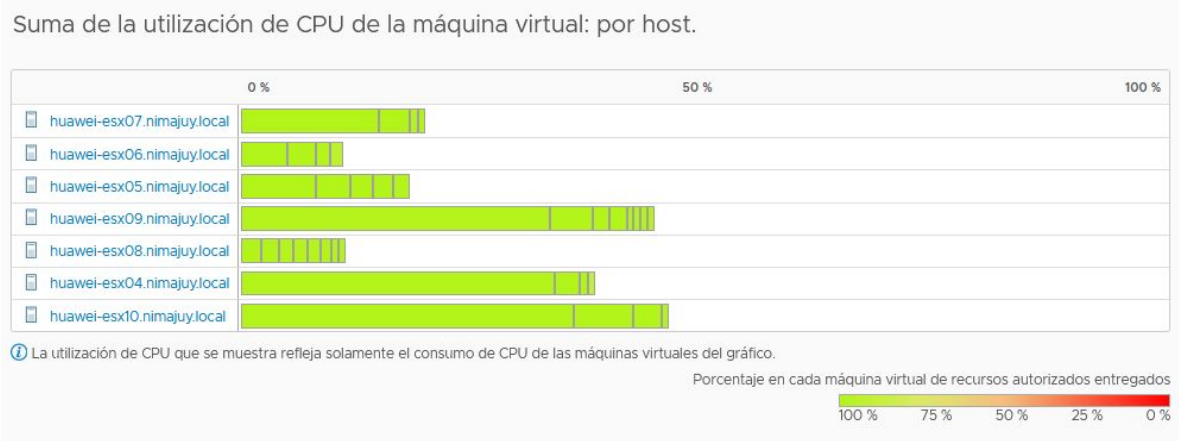


Figura 8. Consumo CPU en el Cluster de Base de datos.

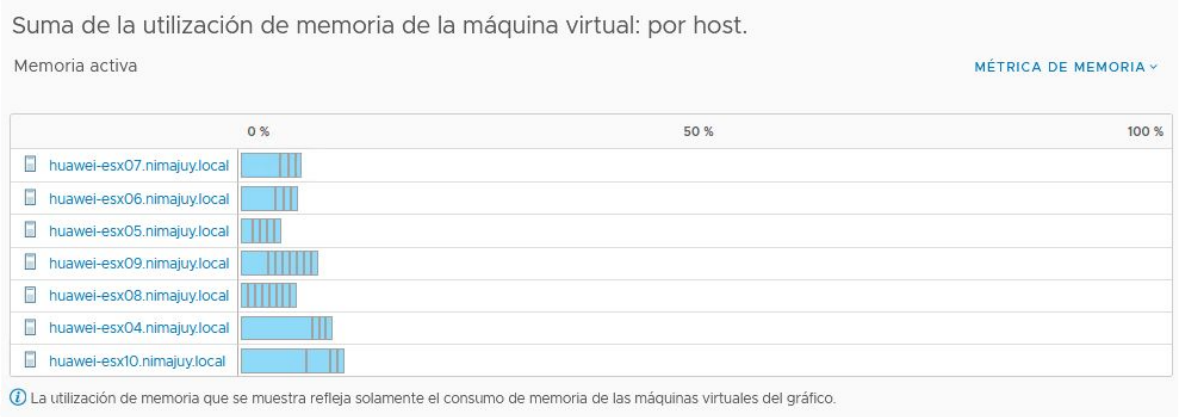


Figura 9. Consumo de Memoria en el Cluster de Base de datos.

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 octubre y su clasificación.

Tabla 16. Casos registrados en el mes de octubre 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 octubre el porcentaje de disponibilidad de servicio fue de 100%.

$$Disponibilidad = \left(1 - \frac{0}{30 * 24horas * 60minutos}\right) * 100\% = 100\%$$

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 OCTUBRE 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 406 días y el equipo Servidor en un tiempo de operación desde los últimos 177 días.

Name	IP Address	Module Role	Health	Last Status Updated
ELNFSS.ENLANUBE.COM.CO	10.99.93.120	Super	Normal	Nov 01 2022, 10:52:34 AM

Organization	Name	IP Address	Health	Uptime	Last Status Updated
Adres	CollectorAdres	10.90.54.10	Normal	406d 22h	Nov 01 2022, 10:55:46 AM

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 Octubre del 2022. **Los servidores Windows no están reportando por WMI, esto puede deberse a una falla de credenciales sobre el usuario creado para el protocolo, por lo cual se debe realizar la actualización del collector para realizar la integración nuevamente.**

Name	IP	Device Type	Status	Discovered	Method
AdresFSCo	10.90.54.10	CentOS Linux	Approved	Sep 20 2021, 12:57:53 PM	LOG
APPINT01.adres.gov.co	192.168.60.2	Windows Server 2019	Approved	Sep 27 2022, 06:21:08 PM	SNMP, PING
APPWEB01.adres.gov.co	192.168.70.201	Windows Server 2019	Approved	Sep 27 2022, 06:24:56 PM	SNMP, 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 Octubre 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, se observa que ningún dispositivo presento una alta indisponibilidad por lo cual se cuenta con un SLA de 100%, sin embargo se presentó un tiempo indisponible de 1 minuto, lo cual se debió a un reinicio en el supervisor del SIEM que se llevó a cabo en la actualización del mismo.

Host Name	Current Uptime	Total Downtime	Achieved Uptime (SLA)
APPINT01.adres.gov.co	25d 4h	1m 3s	100
APPWEB01.adres.gov.co	25d 4h	31s	100

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

5. USO DE COMPONENTES

5.0 Uso de licenciamiento

Del licenciamiento habilitado para el cliente ADRES de una tasa de eventos mínima de 6,85EPS y un máximo de hasta 392 EPS, en promedio diariamente se están utilizando 100 EPS generado por los 4 dispositivos integrados.

Rank	License Attribute	Allowed (per License)	Current Usage
1	Total EPS	200	see below
2	Devices	10	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	FIMS	Not Specified	0

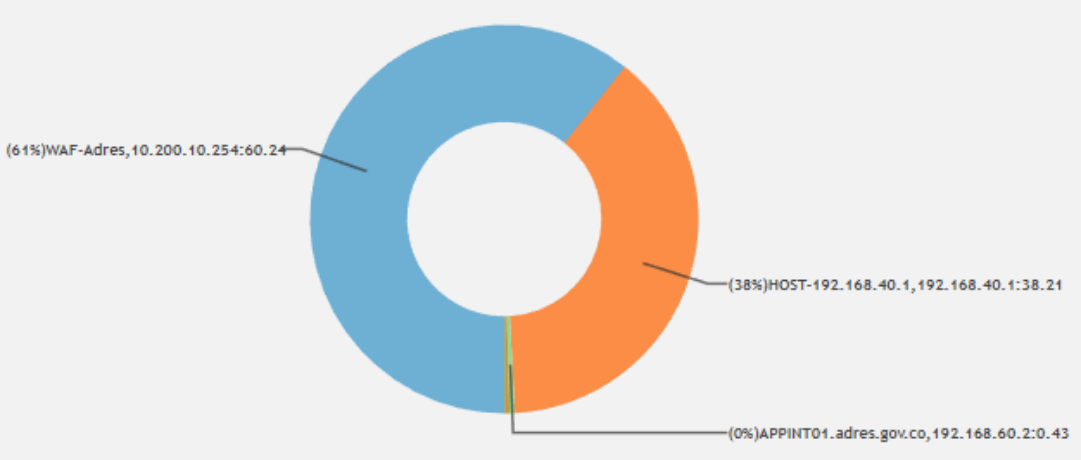
Rank	Organization ID	Reporting IP	AVG(Event Rate)	MAX(Event Rate)	MIN(Event Rate)
1	2001	10.90.54.10	100.71	392.93	6.85

Ilustración 4 Uso de licenciamiento durante el mes de Octubre 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	60.24
HOST-192.168.40.1	192.168.40.1	38.21
APPINT01.adres.gov.co	192.168.60.2	0.43
APPWEB01.adres.gov.co	192.168.70.201	0.42

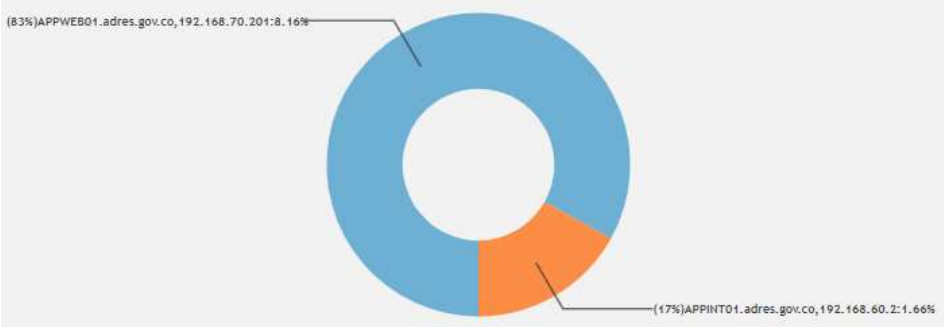
Ilustración 5 Tasa de eventos por dispositivos durante el mes de Octubre 2022.

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:



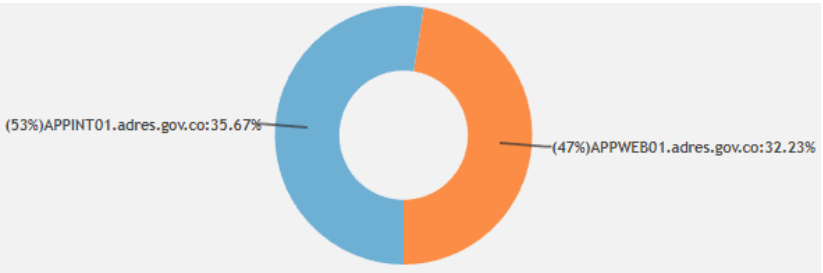
Host Name	Host IP	AVG(CPU Util)	MAX(CPU Util)	MIN(CPU Util)
APPWEB01.adres.gov.co	192.168.70.201	8.16%	96.56%	0.88%
APPINT01.adres.gov.co	192.168.60.2	1.66%	29.44%	0.00%

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

Se verifica que los dispositivos no cuentan con consumos críticos de CPU en promedio, se evidencias caídas fuertes de CPU y un uso eventual de hasta el 96% de consumo máximo 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	AVG(Memory Util)	MAX(Memory Util)	MIN(Memory Util)
APPINT01.adres.gov.co	35.67%	73.09%	5.02%
APPWEB01.adres.gov.co	32.23%	67.83%	3.16%

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

Se verifica que los dispositivos cuentan con un consumo promedio estable, pero se han presentado consumos altos de un 73% para el APPINT01.

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 e IPS:

Destination IP	Event Name	COUNT
10.200.10.158	Gh0st.Rat.Botnet	10
10.200.10.158	Bladabindi.Botnet	10
10.200.10.158	Mirai.Botnet	5
10.200.10.158	RedXOR.Botnet	4
192.168.70.32	Mirai.Botnet	2
10.200.10.158	Mirai.Botnet	2
10.200.10.157	Gh0st.Rat.Botnet	2
10.200.10.157	Bladabindi.Botnet	2
10.200.10.157	FortiGate ips malicious url	2
10.200.10.157	FortiGate ips malicious url	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	1

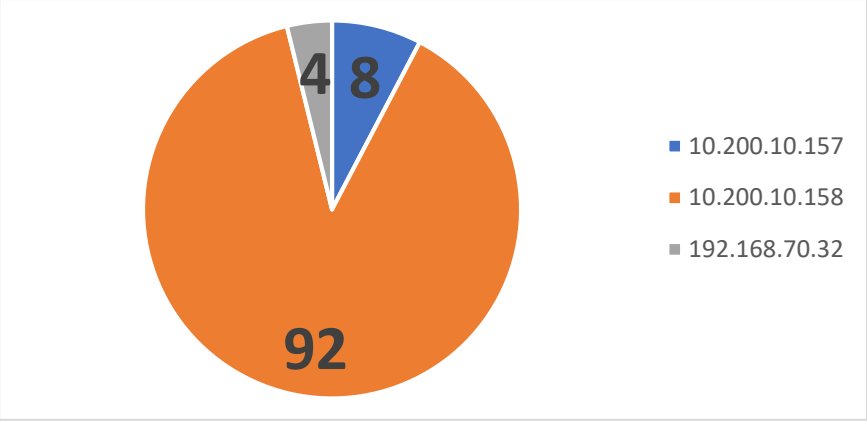


Ilustración 8 Top de IPs con malware reportados durante el mes de Octubre 2022

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.

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:

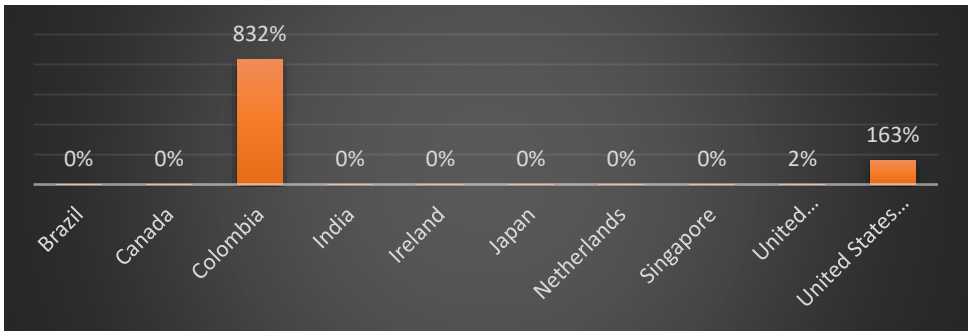


Ilustración 9 Top países de tráfico permitido durante el mes de Octubre 2022

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:

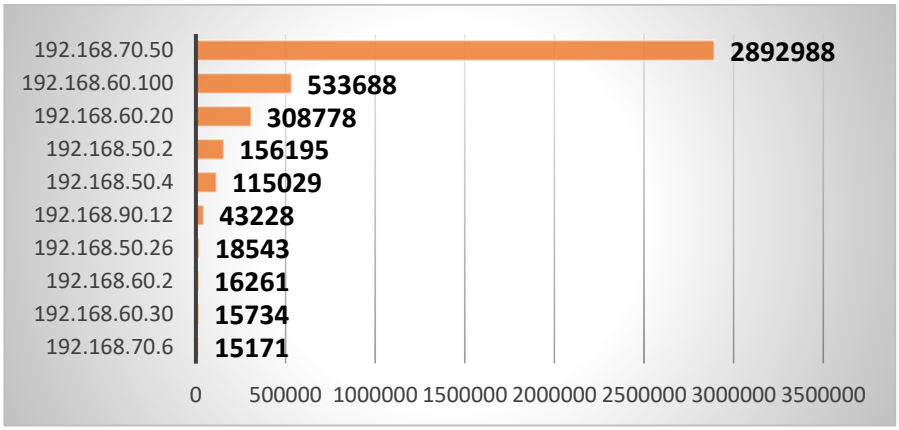


Ilustración 10 Top fuentes con más bloqueos reportados durante el mes de Octubre 2022

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:

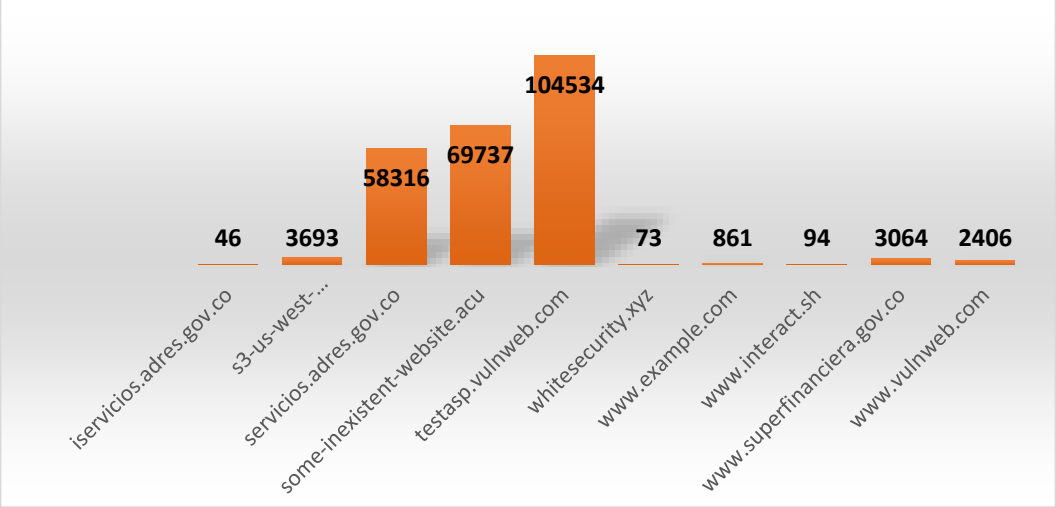


Ilustración 11 Top de categorías con más bloqueos reportados durante el mes de Octubre 2022

En la siguiente imagen podremos encontrar las categorías y páginas visitadas más relevantes, en donde observamos que el mayor destino fue http://testasp.vulnweb.com/, la cual corresponde a un sitio para probar el escáner de vulnerabilidades web de Acunetix

7.4 Firewall: Top de cambios realizados

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

Firewall Action	admin	frojasv	No usuario	FGT_ha_admin	Total general
Add	81,82%	18,18%	0,00%	0,00%	100,00%
Delete	33,33%	66,67%	0,00%	0,00%	100,00%
Edit	72,97%	24,32%	0,00%	2,70%	100,00%
Move	88,89%	11,11%	0,00%	0,00%	100,00%
update	0,00%	0,00%	100,00%	0,00%	100,00%
Total general	**13,91%**	**3,97%**	**81,90%**	**0,22%**	**100,00%**

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

Se puede observar que el 81% de los cambios realizados son por actualización, seguido por el 13,91% de cambios realizados por el usuario admin y un 3,97% de cambios realizados por el usuario frojasv, se recomienda validar los cambios a nivel de eliminación y traspaso.

8. INCIDENTES

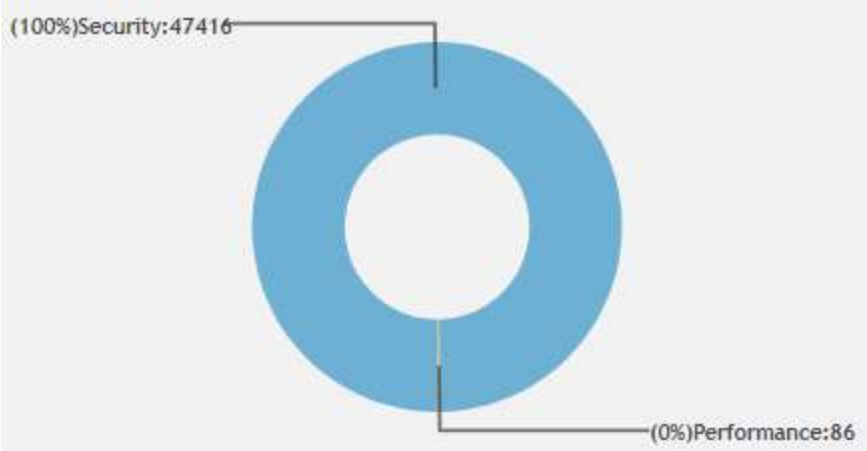
8.0 Vista Global

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 100% es asociada a la categoría de Security, seguido por la categoría de disponibilidad con el 0% y la categoría de performance con el 0%.



Incident Category	Count
Security	47,416
Performance	86
Availability	60
Change	3

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

Event Name	Event Severity	Severity Category	Count
Server Down: No Ping Response	10	HIGH	25
Missing specific performance metric from a device	10	HIGH	16
Server Degraded: Lossy Ping Response	8	MEDIUM	1
Sudden Decrease in Reported Events From A Host	7	MEDIUM	12
Service Degraded: Slow Response to STM: Has IP	7	MEDIUM	4
No logs from a device	7	MEDIUM	2

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

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

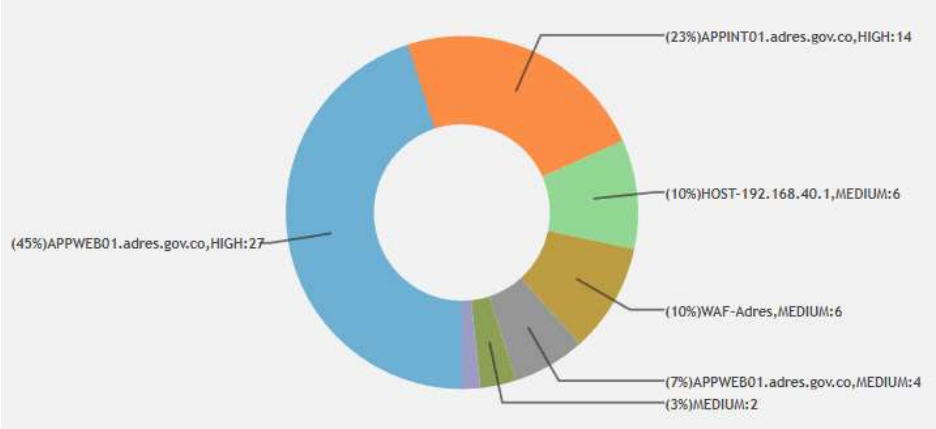


Ilustración 15 Top incidentes de indisponibilidad por dispositivo durante el mes de Octubre 2022.

Se puede observar que el dispositivo con mayor conteo de incidentes de disponibilidad es el dispositivo APPIWEB01 con 31 eventos, seguido del dispositivo APPINT01 con 30 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.

☑	Server Down: No Ping Response	10	HIGH	25
☑	Missing specific performance metric from a device	10	HIGH	16

- **Server Down: No Ping Response**
  Detecta que un dispositivo no responde al ping: se pierden 10 de cada 10 paquetes de ping: el incidente se puede levantar por falla de enrutamiento con el dispositivo, la mayor parte se presentó durante un reinicio aplicado al supervisor durante la actualización del mismo, el incidente Missing Specific obedece a la misma razón.

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 Octubre 2022.

Event Name	Event Severity	Severity Category	Count
Server Disk Space Critical	9	HIGH	31
Sudden Increase in STM Response Times	7	MEDIUM	16
Sudden Increase in Network Interface Errors	7	MEDIUM	12
Server Disk space Warning	5	MEDIUM	8
Sudden Increase in SNMP Response Times	7	MEDIUM	7
Sudden Increase in System Memory Usage	7	MEDIUM	6
Sudden Increase in Server Process Count	7	MEDIUM	2
Sudden Increase in Ping Response Times	7	MEDIUM	2
Sudden Increase In System CPU Usage	7	MEDIUM	1
Server CPU Warning	5	MEDIUM	1

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

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

Host Name	Severity Category	Event Severity	Event Name	Count
APPINT01.adres.gov.co	HIGH	9	Server Disk Space Critical	27

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

Se puede observar que el dispositivo con mayor conteo de incidentes de rendimiento es el dispositivo APPINT01 con 27 eventos.

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.

- **Server Disk Space Critical**: El incidente obedece al disco L:\Log1 del equipo APPINT01, el cual no tiene espacio disponible.

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 Octubre 2022.

Event Name	Severity Category	Event Severity	Count
Inappropriate Website access	MEDIUM	7	45,573
Stealth Scan	HIGH	9	984
Inappropriate Website access: High volume	HIGH	9	310
System Exploit Detected by Network IPS	MEDIUM	7	131
Large Outbound Transfer To Outside My Country	MEDIUM	8	101
Multiple IPS Detected Scans From Same Src	MEDIUM	7	82
Large Outbound Transfer	MEDIUM	8	65
Successful VPN Logon From Outside My Country	MEDIUM	8	53
Sudden Increase In Permitted Traffic To Host	MEDIUM	7	16
Privilege Escalation Exploits	MEDIUM	7	15

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

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

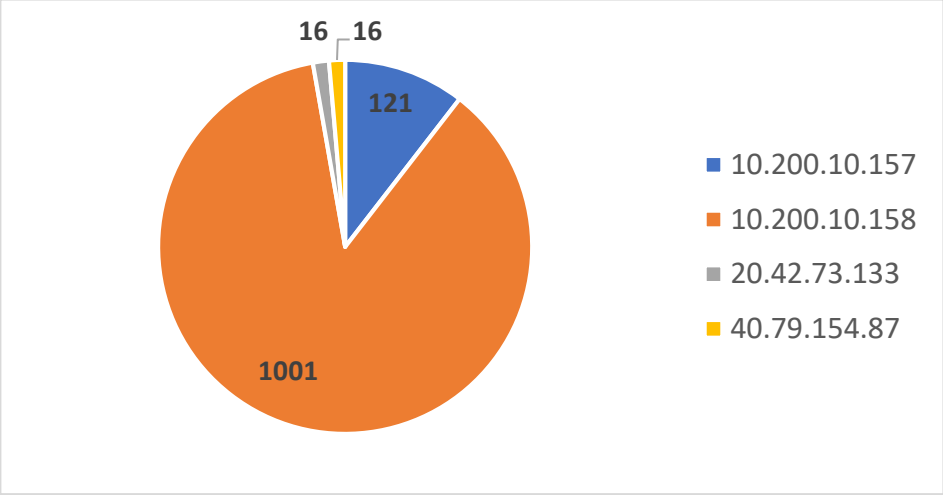


Ilustración 19 Top incidentes de seguridad por dispositivo durante el mes de Octubre 2022.

Se puede observar que el dispositivo con mayor conteo de incidentes de seguridad es el dispositivo con IP 10.200.10.158, con 1001 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, para **inapropiate website acces**, adjunto el archivo Excel el cual contiene la información de páginas visitadas y dispositivos que lo generan.

- **Stealth Scan**: Podemos validar que el target con mayor número de ataques es la ip 10.200.10.158, del total de los 1116 ataques de los cuales se permitieron 127.

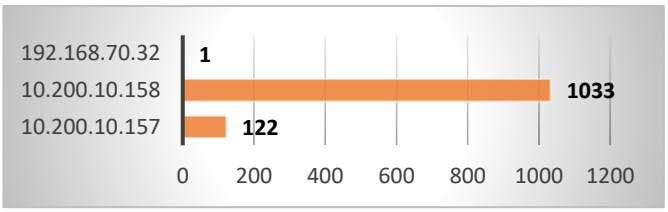


Ilustración 20 Top incidentes de Stealth Scan por dispositivo durante el mes de Octubre 2022.

Evento	Deny	Permit	Total
Cisco.Smart.Install.Feature.Enable.Scanner		5	5
Nmap.Script.Scanner	104	1	105
PHP.Diescan	1		1
ZGrab.Scanner	892	120	1012
Muieblackcat.Scanner	2		2
Masscan.Scanner	28	1	29
Nessus.Scanner	1		1
Acunetix.Web.Vulnerability.Scanner	1		1
Total	1029	127	1156

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

- **System Exploit Detected by Network IPS:** Detecta un exploit detectado por IPS (por ejemplo, desbordamiento de búfer, escalada de privilegios) precedido opcionalmente por un reconocimiento. A continuación se validaran los países desde donde son detectados los ataques.

Etiquetas de fila	Source Country
China	65
Germany	10
India	24
Italy	12
Korea (the Republic of)	8
Netherlands	10
Russian Federation	6
Switzerland	6
United Kingdom of Great Britain and Northern Ireland	24
United States of America	63
Colombia	16
Total general	**244**

A continuación se validan las firmas de los exploit, los cuales fueron denegados por el Firewall.

Firma	Total
Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	6
Dasan.GPON.Remote.Code.Execution	34
D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	41
Java.Debug.Wire.Protocol.Insecure.Configuration	11
MS.Windows.HTTP.sys.Request.Handling.Remote.Code.Execution	7
NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	29
PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	23
TrueOnline.ZyXEL.P660HN.V1.Unauthenticated.Command.Injection	90
VACRON.CCTV.Board.CGI.cmd.Parameter.Command.Execution	9
Apache.Log4j.Error.Log.Remote.Code.Execution	18
Total general	**268**

Ilustración 22 Top incidentes de System Exploit Detected por firmas durante el mes de Octubre 2022.

9. ACTIVIDADES ADICIONALES RELEVANTES DEL MES

Los cambios reportados obedecen a la actualización del supervisor, pasando de la versión 6.3.2 a la versión 6.6.2, así mismo se realizó actualización del protocolo SNMP para los dispositivos servidores.

10. ACCIONES DE MEJORA

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 y países desde donde se realiza la el escaneo indicadas en la presentación, ya que la acción de la regla fue **permitida,** incluir la firma Cisco.Smart.Install.Feature.Enable.Scanner y ZGrab.Scanner ya que dichos 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. Se realizara una actualización del collector para así poder actualizar el protocolo de integración WMI de los servidores Windows.

Tabla 15. Casos reportados en el mes octubre 2022

INFORME DE CASOS REGISTRADOS - SERVICIOS DE DATACENTER

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

PERÍODO: 01/10/2022 - 31/10/2022

No.	Tipo	Fecha Inicio	Hora Inicio	Canal	Solicitante	Asunto	Fecha de cierre	Hora cierre	Responsable	Solución	Indisponibilidad servicio	Tiempo indisponibilidad	% Disponibilidad
1861	Solicitud de servicio	4/10/2022	7:58 a.m.	Correo	Enlanube	Configuración regla XROAD SDS	5/10/2022	12:29 p.m.	Juan Manuel Rojas	04/10/2022 9:22 a.m. De acuerdo a la solicitud realizada, me encuentro ejecutando la configuración en el firewall, 05/10/2022 12:29 p.m. Se realiza con éxito la configuración solicitada en el firewall	NO	0	100,00%
1866	Solicitud de servicio	4/10/2022	1:53 p.m.	Correo	Enlanube	Configuración regla XROAD MINSALUD PROD	5/10/2022	12:36 p.m.	Juan Manuel Rojas	Se realiza con éxito la configuración solicitada en el firewall:	NO	0	100,00%
1870	Solicitud de servicio	5/10/2022	8:02 a.m.	Correo	Enlanube	Validación y ajuste WAF	13/10/2022	8:53 a.m.	Juan Manuel Rojas	05/10/2022 12:42 p.m. Confirmo mi asistencia a la sesión, 13/10/2022 8:53 a.m. Se realizo sesión con los ingenieros Fabian Bernal y Wilmer Hernández de ADRES a la hora programada para la validación de un bloqueo presentado en WAF, el cual fue reportado por un usuario, el usuario no se encontraba en sitio, por lo cual no fue posible realizar las pruebas con este usuario, el ingeniero Fabian realiza la prueba con un usuario que tiene, pero no se presenta el bloqueo reportado, Los ingenieros Fabian Bernal y Wilmer Hernández indican realizaran validaciones con otros usuarios y cualquier novedad nos será informada para continuar con la validación.	NO	0	100,00%
1872	Solicitud de servicio	5/10/2022	8:17 a.m.	Correo	Enlanube	Protección WAF - Fortiguard Expirada	5/10/2022	8:19 a.m.	Javier Orejarena	Buenos días. Creo que En La Nube es quien suministra los dispositivos Fortinet y tendría entonces la potestad para comprar la renovación de esas licencias.	NO	0	100,00%
1881	Solicitud de servicio	5/10/2022	4:04 p.m.	Correo	Enlanube	Informe de Backups	5/10/2022	5:16 p.m.	Angie Ramírez	Informe de Backups	NO	0	100,00%
1895	Solicitud de servicio	7/10/2022	8:58 a.m.	Correo	Enlanube	Aumento disco APPWEB01 192.168.70.2	7/10/2022	2:22 p.m.	Javier Orejarena	Buenas tardes, se aumenta la capacidad del disco G: a 500 GB.	NO	0	100,00%
1890	Solicitud de servicio	7/10/2022	11:53 a.m.	Correo	Enlanube	PARCHES DE ACTUALIZACION SERVIDORES - SEPTIEMBRE # 5	16/10/2022	10:00 p.m.	Mario Merlini	08/10/2022 8:01 p.m. se da inicio a la tarea de reinicio tras la instalación de actualizaciones de las máquinas enumeradas a continuación 8:12 p.m. se da fin a la tarea de reinicio tras la instalación de actualizaciones de las máquinas enumeradas a continuación. 11/10/2022 7:03 p.m. se da inicio a la tarea de reinicio tras la instalación de actualizaciones de las máquinas enumeradas a continuación. 7:25 p.m. se da fin a la tarea de reinicio tras la instalación de actualizaciones de las máquinas enumeradas a continuación. 13/10/2022 8:30 p.m. se da inicio a la tarea de reinicio tras la instalación de actualizaciones de las máquinas enumeradas a continuación. 9:01 p.m. se da inicio a la tarea de reinicio tras la instalación de actualizaciones de las máquinas enumeradas a continuación. 9:17 p.m. se da fin a la tarea de reinicio tras la instalación de actualizaciones de las máquinas enumeradas a continuación 9:52 p.m. se da inicio a la tarea de reinicio tras la instalación de actualizaciones de las máquinas enumeradas a continuación. 16/10/2022 8:30 p.m. se da inicio a la tarea de reinicio tras la instalación de actualizaciones de las máquinas enumeradas a continuación. 8:42 p.m. se da fin a la tarea de reinicio tras la instalación de actualizaciones de las máquinas enumeradas a continuación. 16/10/2022 9:00 p.m. se da inicio a la tarea de reinicio tras la instalación de actualizaciones de las máquinas enumeradas a continuación. 9:28 p.m. se da fin a la tarea de reinicio tras la instalación de actualizaciones de las máquinas enumeradas a continuación. 9:30 p.m. se da inicio a la tarea de reinicio tras la instalación de actualizaciones de las máquinas enumeradas a continuación. 10:00 pm se da fin a la tarea de reinicio tras la instalación de actualizaciones de las máquinas enumeradas a continuación.	NO	0	100,00%
1908	Solicitud de servicio	10/10/2022	8:15 a.m.	Correo	Enlanube	Modificación VPN y regla FW-	10/10/2022	10:31 a.m.	Juan Manuel Rojas	10/10/2022 9:51 a.m. La solicitud esta siendo atendida, 10/10/2022 10:31 a.m. Se crea el objeto BDTREP01 - 192.168.90.14	NO	0	100,00%
1910	Solicitud de servicio	10/10/2022	9:08 a.m.	Correo	Enlanube	Limitacion IP´s Colombia FW - 192.168.60.10	10/10/2022	10:09 a.m.	Juan Manuel Rojas	10/10/2022 9:50 a.m. La solicitud está siendo atendida, 10:09 a.m. Se realiza la configuración solicitada para las reglas 50, 77 y 103:	NO	0	100,00%
1916	Solicitud de servicio	10/10/2022	3:04 p.m.	Correo	Enlanube	Restauración de archivos BDPERP01 diario del 6-7 de octubre 2022	10/10/2022	5:31 p.m.	Mario Merlini	10/10/2022 3:30 p.m. Buenas tardes Ingenieros, se da inicio a la restauración de los archivos requeridos. 5:31 p.m. se informa que los archivos solicitados para restauración ya se encuentran en las carpetas asignadas. Restore tomado del backup:	NO	0	100,00%
1936	Solicitud de servicio	11/10/2022	1:58 p.m.	Correo	Enlanube	Configuración VPN Site to Site GLOBAL HITSS	12/10/2022	12:23 p.m.	Juan Manuel Rojas	11/10/2022 5:04 p.m. El requerimiento está siendo procesado, 12/10/2022 12:23 p.m. Con respecto a la solicitud realizada, se realiza la creación del túnel vpn, adicional a esto en comunicación con el ingeniero Fabian Bernal de ADRES, se programa sesión para mañana en la cual se realizarán validaciones,	NO	0	100,00%
1964	Solicitud de servicio	13/10/2022	1:55 p.m.	Correo	Enlanube	Configuración regla FW - XROAD SDS PROD	13/10/2022	2:51 p.m.	Juan Manuel Rojas	Se realiza la configuración solicitada sobre la regla 85 en el firewall,	NO	0	100,00%
1991	Solicitud de servicio	18/10/2022	11:42 a.m.	Correo	Enlanube	Eliminación maquina APPTFS02 - 192.168.60.38	19/10/2022	11:17 a.m.	Javier Orejarena	18/10/2022 12:05 p.m. Buenas tardes, acabamos de recibir esta solicitud, será borrada hoy 11:59 pm 19/10/2022 11:17 a.m. Buenos días, tal como recibieron la confirmación en el correo de hoy la máquina virtual fue borrada.	NO	0	100,00%

1998	Solicitud de servicio	18/10/2022	3:05 p.m.	Correo	Enlanube	Aprovisionamiento VM APTERP02 192.168.90.58	21/10/2022	10:41 a.m.	Javier Orejarena	18/10/2022 3:39 p.m. Buenas tardes, por favor confirmar la versión de Windows Server (piden 2016 pero es posible que necesiten una más reciente). 21/10/2022 10:41 a.m. la máquina virtual APTERP02 con ip 192.168.90.58 ya fue desplegada con los requerimientos hechos en este correo. Queda pendiente que de parte de ADRES la agreguen al dominio adres.gov.co	NO	0	100,00%
2053	Solicitud de servicio	21/10/2022	11:11 a.m.	Correo	Enlanube	Unidad almacenamiento BDTERP01 - 192.168.90.34	21/10/2022	12:09 p.m.	Javier Orejarena	Buenas tardes, la unidad G – NUEVO con 2 TB ya fue aprovisionada de acuerdo con la solicitud.	NO	0	100,00%
2081	Solicitud de servicio	25/10/2022	10:48 a.m.	Correo	Enlanube	Lentitud BDPMRE01 - 192.168.50.42	26/10/2022	5:40 p.m.	Javier Orejarena	25/10/2022 10:59 a.m. Buenos días. Respecto al server BDPMRE01 observamos que inició su tarea de backup esta madrugada a las 00:24 am y en este momento está en proceso de consolidación de sus discos y remoción del último snapshot creado. Como es un servidor muy grande (tiene 20 TB de almacenamiento) y posiblemente se estaba ejecutando algún proceso intensivo en disco vemos que el proceso final de remoción del snapshot está tomando bastante tiempo y no se puede interrumpir ni cancelar. Tenemos que esperar a que lo termine y es posible que para evitar futuros inconvenientes como éste se tenga que re-evaluar la hora del backup, el método del backup (hacerlo solo con snapshots) o el tamaño de la máquina virtual. 26/10/2022 5:40 p.m. Buenas tardes, la consolidación de los discos de la máquina virtual finalizó 3pm de hoy sin novedades, esperamos que el rendimiento de la máquina virtual se haya restablecido.	NO	0	100,00%
2991	Solicitud de servicio	25/10/2022	4:03 p.m.	Correo	Enlanube	Lentitud BDPBDU01 - 192.168.50.10	25/10/2022	4:44 p.m.	Angie Ramírez	Se realiza la validación de la máquina en mención y se evidencia que está leyendo datos a 1.5 GB/s y escribiéndolos a unos 300 MB/s.	NO	0	100,00%
2095	Solicitud de servicio	26/10/2022	7:20 a.m.	Correo	Enlanube	Solicitud APPSER02 - 192.168.60.22	26/10/2022	7:36 a.m.	Javier Orejarena	se aprovisiona la unidad D: con etiqueta NUEVO6 de 2 TB de acuerdo con el requerimiento. Ya se agotaron las letras de unidades de disco en esta máquina, se tuvo que remover la letra de unidad del DVD para asignarlo a la máquina.	NO	0	100,00%
2100	Solicitud de servicio	26/10/2022	11:13 a.m.	Correo	Enlanube	Eliminación maquina APPSGD06 - 192.168.60.44	26/10/2022	8:53 p.m.	Javier Orejarena	Buenas noches, procedemos a la eliminación de la máquina virtual solicitada.	NO	0	100,00%
2101	Solicitud de servicio	26/10/2022	11:34 a.m.	Correo	Enlanube	Aprovisionamiento VM APP	27/10/2022	9:21 a.m.	Javier Orejarena	se completó el despliegue de la máquina virtual APPLOG01 con S.O. Debian 10 en la ip 192.168.60.44 Para acceder a ella por SSH por favor utilizar los usuarios root y admcliente, ambos están asignados con la misma clave de siempre.	NO	0	100,00%
2101	Solicitud de servicio	26/10/2022	2:41 p.m.	Correo	Enlanube	Configuración VPN Site to Site Alfapeople	28/10/2022	2:14 p.m.	Juan Manuel Rojas	26/10/2022 3:08 p.m. La solicitud esta en proceso 28/10/2022 2:14 p.m. El día miércoles (26/10/2022) se realizo la creación en el firewall fortigate de la VPN site to site para el cliente Alfapeople: El día de ayer (27/10/2022) se realizó sesión con personal de ADRES y Alfapeople, en donde se validó la configuración de la vpn y el correcto funcionamiento de la misma, quedando esta funcional:	NO	0	100,00%
2126	Solicitud de servicio	28/10/2022	11:08 a.m.	Correo	Enlanube	VPN Nombra a 192.168.60.44	31/10/2022	10:52 a.m.	Juan Manuel Rojas	28/10/2022 La solicitud esta en proceso 31/10/2022 10:52 a.m. Se realiza la creación del usuario y de la vpn solicitada: Se realizan pruebas de conexión, siendo estas exitosas: Se habilita la opción de una sesión por usuario al tiempo para esta vpn:	NO	0	100,00%