	PROCESO	GESTIÓN DE CONTRATACIÓN	CÓDIGO	GCON-FR01
	FORMATO	INFORME DE CUMPLIMIENTO DE AVANCES DE OBLIGACIONES CONTRACTUALES Y PAGO	VERSIÓN	03
			FECHA	10/05/2021

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	1/11/2022	Hasta	30/11/2022
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.



Firma del Contratista

Fecha: 5/12/2022

	PROCESO	GESTIÓN DE CONTRATACIÓN	CÓDIGO	GCON-FR01
	FORMATO	INFORME DE CUMPLIMIENTO DE AVANCES DE OBLIGACIONES CONTRACTUALES Y PAGO	VERSIÓN	03
			FECHA	10/05/2021

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	\$ 2.744.351.557,65	\$313.300.000	\$0	\$105.341,83

La ADRES cancelará al CONTRATISTA, la suma de trescientos trece millones trescientos mil pesos (\$313.300.000)

PAGO DE SEGURIDAD SOCIAL PERSONAS NATURALES

Mes de ejecución contractual

CONCEPTO	PLANILLA No.	VALOR	PERIODO		FECHA DE PAGO
			DESDE	HASTA	
Salud	63541039	\$683.986.600	1/12/2022	31/12/2022	29/11/2022
Pensión			1/11/2022	31/11/2022	29/11/2022
ARL			1/11/2022	31/11/2022	29/11/2022

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:

- 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.
- 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.

	PROCESO	GESTIÓN DE CONTRATACIÓN	CÓDIGO	GCON-FR01
	FORMATO	INFORME DE CUMPLIMIENTO DE AVANCES DE OBLIGACIONES CONTRACTUALES Y PAGO	VERSIÓN	03
			FECHA	10/05/2021

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	<ol style="list-style-type: none"> 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-170 4. En caso de primer pago debe aportar: <ol style="list-style-type: none"> a. Los soportes relacionados en el formato de deducciones para efectos de retención en la fuente.

En constancia, firmo:



Ing. Carlos Andres Ruiz Romero
C.C. 86.051.326 de Villavicencio

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., 7/12/2022

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



ADRES	PROCESO	GESTIÓN DE CONTRATACIÓN	CÓDIGO	GCON-FR02
	FORMATO	INFORME DE CUMPLIMIENTO Y PAGO FINAL.	VERSIÓN	03
			FECHA	10/05/2021

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	CARLOS ANDRES RUIZ ROMERO	CARLOS ANDRES RUIZ ROMERO
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 Acuerdo 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	1/11/2022	Hasta	30/11/2022
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	No aplica			
Cesión	No aplica			
Terminación	finalización de seguimiento del contrato			

INFORME DE EJECUCIÓN ECONÓMICA Y FINANCIERA

CONCEPTO	VALOR
Valor inicial del Contrato o Convenio	\$ 3.870.492.180,80
Valor adiciones	\$ 2.161.974.716,62
Valor total incluidas las adiciones	\$ 6.032.466.897
Valor pagado o desembolsado al Contratista.	\$ 5.838.551.045
Valor Pendiente por pagar al Contratista	\$ 313.300.000
Valor para reintegrar o reintegrado por parte del Contratista.	\$ 0
Valor a liberar	\$ 105.341,83
Valor liberado	\$ 1.039.953.063,33
Valor total ejecutado	\$ 6.151.851.045,35

INFORME DE EJECUCIÓN

Para garantizar el cumplimiento del objeto del contrato, según lo pactado, el contratista constituyó garantía única de cumplimiento con la Compañía de Seguros Aseguradora Solidaria de Colombia como sigue:

PÓLIZA No.	AMPAROS	VALORES ASEGURADOS	VIGENCIAS	
			FECHA INICIO	FECHA FINAL
2674817-1	Cumplimiento	\$967.623.045,20	3/08/2020	31/05/2025

Trámites Sancionatorios (Si aplica)

OBLIGACION(ES) INCUMPLIDA(S)	TRÁMITE
No aplica	No aplica

INFORME DE EJECUCIÓN TÉCNICA

En el evento que la forma de pago se haya pactado por % de ejecución deberá diligenciar el siguiente cuadro para cada caso:

OBLIGACIÓN	PORCENTAJE DE EJECUCIÓN	CAUSAS	ACCIONES ADOPTADAS

Existen obligaciones específicas pos-ejecución (Aquella obligación que se extiende más allá del plazo de ejecución y/o de liquidación):

SI NO

En caso afirmativo relacionar las obligaciones:

OBLIGACIÓN	FECHA DE CUMPLIMIENTO	FECHA DE VERIFICACIÓN (*)

DESARROLLO DEL CONTRATO O CONVENIO

- El contratista presentó informes de ejecución de las actividades a su cargo, los cuales contaron con el visto bueno del Supervisor(a), de la siguiente manera:

- a) Del período comprendido entre el 1/11/2020 al 30/11/2020
- b) Del período comprendido entre el 1/12/2020 al 31/12/2020
- c) Del período comprendido entre el 1/1/2021 al 31/1/2021
- d) Del período comprendido entre el 1/2/2021 al 28/2/2021
- e) Del período comprendido entre el 1/3/2021 al 30/3/2021
- f) Del período comprendido entre el 1/4/2021 al 31/4/2021
- g) Del período comprendido entre el 1/5/2021 al 30/5/2021
- h) Del período comprendido entre el 1/6/2021 al 31/6/2021
- i) Del período comprendido entre el 1/7/2021 al 30/7/2021
- j) Del período comprendido entre el 1/8/2021 al 31/8/2021
- k) Del período comprendido entre el 1/9/2021 al 30/9/2021
- l) Del período comprendido entre el 1/10/2021 al 31/10/2021
- m) Del período comprendido entre el 1/11/2021 al 30/11/2021
- n) Del período comprendido entre el 1/12/2021 al 31/12/2021
- o) Del período comprendido entre el 1/1/2022 al 31/1/2022
- p) Del período comprendido entre el 1/2/2022 al 28/2/2022
- q) Del período comprendido entre el 1/3/2022 al 30/3/2022
- r) Del período comprendido entre el 1/4/2022 al 31/4/2022
- s) Del período comprendido entre el 1/5/2022 al 30/5/2022
- t) Del período comprendido entre el 1/6/2022 al 31/6/2022
- u) Del período comprendido entre el 1/7/2022 al 30/7/2022
- v) Del período comprendido entre el 1/8/2022 al 31/8/2022
- w) Del período comprendido entre el 1/9/2022 al 30/9/2022
- x) Del período comprendido entre el 1/10/2022 al 31/10/2022
- y) Del período comprendido entre el 1/11/2022 al 30/11/2022

PROCESO	GESTIÓN DE CONTRATACIÓN	CÓDIGO	GCON-FR02
	FORMATO	INFORME DE CUMPLIMIENTO Y PAGO FINAL.	VERSIÓN 03
			FECHA 10/05/2021

VERIFICACIÓN ENTREGA DE DOCUMENTOS, EQUIPOS Y/O ELEMENTOS

Incluir las obligaciones generales de orden administrativo que implican verificación y entrega de documentos, software, bases de datos, tarjetas de ingreso, carnet, elementos y equipos, etc, de conformidad con los requisitos establecidos para el efecto.


OBLIGACIÓN	VERIFICACIÓN	
	Cumple	No Cumple
Asumir los costos y demás gastos ocasionados con la entrega e instalación de las licencias en cada uno de los equipos requeridos	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reemplazar las licencias en el evento que no cumplan con las especificaciones técnicas exigidas por la ADRES, dentro del día hábil siguiente a la fecha de comunicación que en tal sentido realice la ADRES, a través del supervisor del contrato	<input checked="" type="checkbox"/>	<input type="checkbox"/>
El contratista garantizará el cumplimiento de las condiciones técnicas, jurídicas económicas y comerciales presentadas en la oferta	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Efectuar la entrega del objeto contratado con las características y especificaciones determinadas dentro del término y en el sitio señalado por la ADRES	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Entregar los medios de instalación del software, las licencias y manuales técnicos y de uso de los productos	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Dar soporte y garantía incluyendo las actualizaciones que se liberen del software durante los dos años de suscripción	<input checked="" type="checkbox"/>	<input type="checkbox"/>

De conformidad con lo anterior, LA SUPERVISIÓN CERTIFICA QUE:

1. El (la) Contratista durante el periodo de ejecución del contrato, desarrolló y cumplió con las obligaciones generales especificaciones, presentó y entregó los productos y/o informes establecidos en el Contrato o Convenio en mención.
2. Entrego los siguientes productos: El contratista realizó la entrega de las licencias relacionadas en el objeto del contrato, así como el Manual técnico y matriz de escalamiento para el procedimiento de soporte, cumpliendo las característica y especificaciones técnicas exigidas por la entidad
3. Verifique la matriz de riesgos del contrato y se estableció, que no se materializo ninguno de los riesgos

OBSERVACIONES No aplica

En constancia, firma:


 Ing. Carlos Andres Ruiz Romero
 C.C. 86.051.326 de Villavicencio
 Supervisor (es)/Interventor (es)

Lugar y Fecha: Bogotá, D. C., 7/12/2022

**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-170

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

Fecha y hora Factura	
Generación	06/12/2022, 19:37
Expedición	06/12/2022, 19:37
Vencimiento	05/01/2023

Ítem	Descripción	Cantidad	Vr. Unitario	Impto. Cargo	Vr. Total
1	npr03-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	npr03-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	npr03-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	npr03-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	npr03-PaaS - Tomcat - Oro - Alta - Servidor de Uso Estandar - Nube privada - 6.0x o superior - PaaS/M- Cantidad: 13 (Línea No. 5)General	1.00	9,276,925.97	0 %	8,952,233.56
6	npr03-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	npr03-aaS 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	npr03-aaS 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	28,550,862.78	0 %	27,551,582.58
9	npr03-aaS 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	npr03-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	npr03-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	npr03-aaS 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	npr03-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. 13)	1.00	1,180,264.62	0 %	1,138,955.36
14	npr03-aaS 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	npr03-aaS 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	npr03-aaS almacenamiento - Backup de Datos - Alta - Mes - Capacidad: 50TB a <100TB - Almacenamiento SAN - Diario - GB/Mes - Cantidad: 54000 (Línea No. 16)	1.00	3,969,546.91	0 %	3,830,612.77

Ítem	Descripción	Cantidad	Vr. Unitario	Impto. Cargo	Vr. Total
17	npr03-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	npr03-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	npr03-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	npr03-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	npr03-iaaS almacenamiento - Backup de Datos - Alta - Capacidad: 100TB a <200TB - Almacenamiento SAN - Mensual - GB/Mes - Cantidad: 100000 (Linea No. 20)	1.00	7,351,012.79	0 %	7,093,727.34
22	npr03-iaaS almacenamiento - Backup de Datos - Alta - Capacidad: 100TB a <200TB - Almacenamiento SAN - Mensual - GB/Mes - Cantidad: 100000 (Linea No. 21)	1.00	7,351,012.79	0 %	7,093,727.34
23	npr03-iaaS almacenamiento - Custodia de Copias de Seguridad - Cintas LTO2, LTO4, LTO G5, LTO6 LTO7 y LTO8 - Med/M - Cantidad: 60 (Linea No. 22)	1.00	2,119,376.50	19 %	2,447,879.86
24	npr03-iaaS almacenamiento - Custodia de Copias de Seguridad - Cintas LTO2, LTO4, LTO G5, LTO6 LTO7 y LTO8 - Med/M - Cantidad: 60 (Linea No. 23)	1.00	2,119,376.50	19 %	2,447,879.86
25	npr03-Servicios Complementarios - Experto Master - Región 1 - Hora/M - Cantidad: 20 (Linea No. 27)	1.00	226,066.97	0 %	218,154.63
26	npr03-Servicios Complementarios - Experto Master en Base de Datos MSSQL Server - Región 1 - Hora/M - Cantidad: 20 (Linea No. 28)	1.00	226,066.97	0 %	218,154.63
27	npr03-Servicios Complementarios - Arquitecto Master en Computación en la Nube - Región 1 - Hora/M - Cantidad: 20 (Linea No. 29)	1.00	489,811.11	0 %	472,667.72
28	npr03-iaaS Seguridad - Firewall Nueva Generación - Media baja Capacidad - Oro - Hosting físico - Rol de Firewall - 15 Gbps - Sesiones Concurrentes - 7000000 - Mes - Cantidad: 2 (Linea No. 30)	1.00	4,301,577.11	0 %	4,151,021.91
29	npr03-iaaS Procesamiento - Balanceador de Carga Baja Capacidad - Oro - Hosting Físico - Sesiones Capa L4 (entre 1.6 y 14 Millones) - RAM entre 8GB y 32GB - U_Mes - Cantidad: 1 (Linea No. 31)	1.00	1,750,316.15	0 %	1,689,055.08
30	npr03-iaaS Seguridad - Web Application Firewall - Media Capacidad - Oro - Hosting Físico - Desempeño WAF (Mbps) - 500-Mes Cantidad 1 (Linea No. 32)	1.00	1,418,770.76	0 %	1,369,113.78
31	npr03-iaaS Seguridad - Monitoreo y Correlación - Oro - Eventos por segundo (EPS) - por unidad - entre 251 y 500 - Und - Cantidad: 1 (Linea No. 33)	1.00	27,031.22	19 %	31,221.06
32	npr03-iaaS Seguridad - Monitoreo y Correlación - Oro - Eventos por segundo (EPS) - por unidad - entre 251 y 500 - Und - Cantidad: 1 (Linea No. 34)	1.00	13,515,610.84	19 %	15,610,530.52

Total ítems: 32

Valor en Letras:

Doscientos noventa y ocho millones setecientos setenta y ocho mil quinientos cinco pesos m/cte con setenta y tres cent.

Condiciones de Pago:

Crédito - Cuota No. 001 vence el 2023-01-05 por \$ 298,778,505.73

Observaciones:

Observaciones:

Nota: Periodo Servicio Noviembre 2022

Miembro de la Unión Temporal Internexa en la Nube:

1. Internexa SANIT: 811.021.654

2. Infraestructura Virtual SASNIT: 900.486.933

Por favor tener en cuenta el siguiente porcentaje de participación de los miembros de la UIT en el presente

Total Bruto	308,273,264.89
IVA 19%	5,026,735.11
Retefuente 3.5%	10,789,564.26
RetelVA 15%	754,010.27
RetelCA 9.66	2,977,919.74
Total a Pagar	298,778,505.73

Por favor tener en cuenta el siguiente porcentaje de participación de los miembros de la SA en el presente:

1. Intemexa SA 8,79%

2 Infraestructura Virtual SAS 91,21%

Intemexa 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%

Intemexa 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: b79f65be2350ecda8c39f51ea9a9dbcbf86b4125c0700bc4a28a1c56371debf3d04ab8a120fce974fcc4f329e09764e5

Información básica de la planilla

Empresa: INTERNEXA S.A.
Tipo Planilla: E
Sucursal o Dependencia: PRINCIPAL
Número de Radicación: 63541039
Fecha de vencimiento: 29/11/2022
Fecha de Pago: 29/11/2022

NIT: 811021654
Periodo liquidación Pensiones: noviembre 2022
Periodo liquidación Salud: diciembre 2022
Total a pagar: \$683,986,600
Total de empleados: 235
Número de Administradoras: 25

Detalles del pago

Razón social recaudo: Compensar OI
Descripción: MiPlanilla.com Pago Proteccion Social
Banco: BANCOLOMBIA
Estado de la transacción: Transacción aprobada

Nit recaudo: 9998600669427
Medio de Pago: Pago Electronico por PSE
Número Autorización: 1781648295

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	235		\$0	\$29,630,600
230201	800229739	Proteccion (ING + Proteccion)	101		\$0	\$148,813,200
230301	800224808	Porvenir	28		\$0	\$42,654,700
230901	800253055	FONDO DE PENSIONES OBLIGATORIAS SKANDIA	10		\$0	\$18,013,800
231001	800227940	Colfondos	13		\$0	\$16,580,300
25-14	900336004	Administradora Colombiana de Pensiones -	74		\$0	\$120,740,200
CCF04	890900841	Comfama Caja de Compensacion Fliar	164		\$0	\$58,742,200
CCF07	890101994	Comfamiliar del Atlantico Caja de Compensacion	2		\$0	\$1,585,100
CCF11	890806490	Caja de Compensacion Familiar de Caldas	1		\$0	\$100,000
CCF24	860066942	Compensar Caja de Compensacion Fliar	56		\$0	\$20,055,800
CCF37	890500516	Comfanorte Caja de Compensacion Fliar	1		\$0	\$100,000
CCF40	890201578	Comfenalco Santander Caja de Compensacion	1		\$0	\$434,500
CCF57	890303208	Comfamiliar Andi Comfandi Caja de	2		\$0	\$974,700
EPS001	830113831	ALIANSA LUD EPS S.A.	4		\$0	\$3,852,500
EPS002	800130907	Salud Total EPS	6		\$0	\$6,418,400
EPS005	800251440	Sanitas EPS	40		\$0	\$35,426,300
EPS008	860066942	Compensar EPS	15		\$0	\$13,399,900

Código	NIT	Administradoras	Num. Afiliados	*Número de incapacidad por riesgos laborales	Valor descontado en incapacidad y/o licencia	Total Pagado
EPS010	800088702	EPS Sura	160		\$0	\$107,885,000
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	5		\$0	\$2,024,200
EPS041	900156264	NUEVA E.P.S. S.A. MOV	1		\$0	\$100,000
ESSC62	900935126	ASMET SALUD EPS SAS	1		\$0	\$125,000
PAICBF	899999239	ICBF Instituto Colombiano de Bienestar Familiar	78		\$0	\$32,704,500
PASENA	899999034	SENA	78		\$0	\$21,804,300
						\$683,986,600

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

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 Intereses 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 FAMILIAR 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

Líneas de Servicio FonoSIMPLE: Bogotá 4446634 - Cali: 554 0515 - Medellín: 514 66 69 - Bucaramanga: 643 80 00 - Cartagena: 694 54 44 - Pereira: 340 25 82 - Barranquilla: 361 88 50 - Resto del País: 018000 971 971 - ¡Más que Fácil, SIMPLE!

SIMPLE S.A. no se hace responsable de las planillas y pagos realizados a través de otros operadores de información dado que no tiene medios para corroborar la veracidad de la misma, su alcance se limita a replicar la información suministrada directamente por el cliente.

Antes de imprimir, asegúrese que sea realmente necesario. Proteger el medio ambiente está en nuestras manos.

¡El Poder de lo SIMPLE!





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-3253-22

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 entre el 1 de junio al 30 de noviembre 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
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	Octubre 2022	Pagado
Noviembre 2022	63541039	683,986,600	Noviembre 2022	Pagado

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

De acuerdo con la Resolución N° 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 30 de noviembre del 2022 la compañía cumplió con la cuota obligatoria de aprendices, dando cumplimiento a lo establecido en la Resolución N° 006720 del 12 de agosto de 2021.

Ernst & Young Audit S.A.S.
Bogotá D.C.
Carrera 11 No 98 - 07
Edificio Pijao Green Office
Tercer Piso
Tel. +57 (601) 484 7000

Ernst & Young Audit S.A.S.
Medellín – Antioquia
Carrera 43A No. 3 Sur-130
Edificio Milla de Oro
Torre 1 – Piso 14
Tel: +57 (604) 369 8400

Ernst & Young Audit S.A.S.
Cali – Valle del Cauca
Avenida 4 Norte No. 6N – 61
Edificio Siglo XXI
Oficina 502
Tel: +57 (602) 485 6280

Ernst & Young Audit S.A.S.
Barranquilla - Atlántico
Calle 77B No 59 – 61
Edificio Centro Empresarial
Las Américas II Oficina 311
Tel: +57 (605) 385 2201



**Building a better
working world**

Sres. Internexa S.A.

Página 2

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: 2022.12.01
12:22:49 -05'00'
Ferney Alonso Cano Vargas
Revisor Fiscal
Tarjeta Profesional 243764-T
Designado por Ernst & Young Audit S.A.S. TR-530

Medellín, Antioquia
1 de diciembre de 2022

Tabla 15. Casos reportados en el mes noviembre 2022

 						INFORME DE CASOS REGISTRADOS - SERVICIOS DE DATACENTER							
						ADRES - Administradora de los Recursos del Sistema General de Seguridad Social en Salud				PERIODO: 01/11/2022 - 30/11/2022			
No.	Tipo	Fecha Inicio	Hora Inicio	Canal	Solicitante	Asunto	Fecha de cierre	Hora cierre	Responsable	Solución	Indisponibilidad servicio	Tiempo indisponibilidad	% Disponibilidad
2194	Solicitud de servicio	1/11/2022	11:36 a.m.	Correo	Enlanube	Creacion VPN Site to Site A2 GB	2/11/2022	2:49 p.m.	Juan Manuel Rojas	Se realiza la creación de la vpn site to site siguiendo los lineamientos indicados en el documento, quedando de la siguiente manera: El día de hoy se realizan pruebas con ADRES y AZURE, quedando la vpn funcional	NO	0	100,00%
2175	Solicitud de servicio	2/11/2022	7:53 a.m.	Correo	Enlanube	Acompañamiento administrador FW	2/11/2022	9:36 a.m.	Juan Manuel Rojas	En sesión realizada por teams, se valida que la VPN site to site creada para el cliente GLOBAL HITSS se encuentra con las dos fases en estado up: Cliente Global Hits reporta inconvenientes para conectarse a los servidores de ADRES por el servicio SQL, una vez se confirma la conectividad por la vpn, indican que procederán a validar el usuario que están utilizando, para descartar falla con el mismo, cualquier novedad será informada,	NO	0	100,00%
2213	Solicitud de servicio	2/11/2022	12:43 p.m.	Correo	Enlanube	Crear caso FW Se solicita generar política de salida para este servicio de alfapeople	2/11/2022	2:40 p.m.	Juan Manuel Rojas	Se realiza la creación de la regla #141 de salida para la vpn del cliente ALFAPEOPLE:	NO	0	100,00%
2253	Solicitud de servicio	4/11/2022	9:01 a.m.	Correo	Enlanube	Revisión configuración FW	8/11/2022	10:25 a.m.	Juan Manuel Rojas	El día viernes 4 de noviembre se realizó sesión por teams con el ingeniero Wilmer de ADRES, se realizó la validación de la configuración en el firewall y se observó que no estaba creada la ruta estática hacia la red 10.90.0.0/23, se realizó la creación de esta ruta estática hacia la red 10.90.0.0/23 como se observa a continuación: Se procede a realizar pruebas de conexión hacia la red 10.90.0.0/23 con acompañamiento del ingeniero Wilmer de ADRES, siendo estas pruebas exitosas.	NO	0	100,00%
05-041122	Solicitud de servicio	4/11/2022	5:36 p.m.	Correo	Enlanube	Editar Regla en FW de DC Se solicita agregar el siguiente puerto 9000 8001 a la regla 134 y 135 08/11/2022 2:34 p.m. Se solicita agregar el siguiente puerto según tabla adjunta a la regla 134 y 135	10/11/2022	11:12 a.m.	Juan Manuel Rojas	08/11/2022 9:56 a.m. Se procede a editar la regla en el firewall según la solicitud realizada: 10/11/2022 11:12 a.m. Se realiza la configuración solicitada en el firewall con las reglas 134 y 135, quedando de la siguiente manera:	NO	0	100,00%
06-081122	Solicitud de servicio	8/11/2022	1:59 p.m.	Correo	Enlanube	Configuración reglas FW	8/11/2022	2:25 p.m.	Juan Manuel Rojas	Se procede a realizar la configuración solicitada en el firewall, Se agregan los puertos 443 y 80 en las reglas 131 y 132: Se agrega el dominio de encriptación a la VPN Site OEl-Soaint:	NO	0	100,00%
07-101122	Solicitud de servicio	10/11/2022	9:38 a.m.	Correo	Enlanube	Acompañamiento administrador FW Solicitamos el acompañamiento del administrador del FW el día de hoy 10 de noviembre a las 11 am. 11/11/2022 8:06 a.m. Solicitamos el acompañamiento del administrador del FW el día de hoy 11 de noviembre a las 10 am.	16/11/2022	2:30 p.m.	Juan Manuel Rojas	10/11/2022 10:11 a.m. Se confirma asistencia 11/11/2022 10:23 a.m. Confirmo mi asistencia a la sesión indicada en el correo precedente. 16/11/2022 2:30 p.m. En conversación con el ingeniero Wilmer de ADRES, informa que la sesión fue cancelada y ya no es requerida,	NO	0	100,00%
08-101122	Solicitud de servicio	10/11/2022	10:59 a.m.	Correo	Enlanube	Eliminación maquina APTFS01 - 192.168.60.26	15/11/2022	8:36 a.m.	Javier Orejarena	Buenos días, la máquina fue eliminada de acuerdo con lo solicitado.	NO	0	100,00%
09-101122	Solicitud de servicio	10/11/2022	11:18 a.m.	Correo	Enlanube	Presentación Maquina APTFAB01 - 192.168.70.40	10/11/2022	4:43 p.m.	Javier Orejarena	Buenas tardes, la máquina APTFAB01 192.168.70.40 ya se encuentra desplegada con los recursos solicitados. Queda pendiente agregarla al dominio adres.gov.co y que ADRES proceda a instalar el SQL Server que requieren. Quedamos atentos a lo que se requiera en este caso.	NO	0	100,00%
10-101122	Solicitud de servicio	10/11/2022	2:06 p.m.	Correo	Enlanube	Renombramiento maquina Se solicita renombrar la maquina BDDFAB01 como BDDTFAB01 en la consola de VMWare	10/11/2022	2:27 p.m.	Javier Orejarena	Buenas tardes, se efectúa el cambio solicitado.	NO	0	100,00%
11-111122	Solicitud de servicio	11/11/2022	4:48 p.m.	Correo	Enlanube	VPN GLOBAL HITSS agregar a dominio de encriptación VPN_ GLOBAL HITSS con su respectiva ruta estática y agregar la una regla de entrada.	15/11/2022	9:59 a.m.	Juan Manuel Rojas	Se realiza la configuración solicitada en la VPN GLOBAL HITSS:	NO	0	100,00%
12-151122	Solicitud de servicio	15/11/2022	9:41 a.m.	Correo	Enlanube	Error reportado en apper01 192.168.60.12 18/11/2022 3:32 p.m. Se valido y se aprobó para el sábado 19/11/2022 hora 9:00 pm a 10:00 pm	19/11/2022	9:21 p.m.	Javier Orejarena	15/11/2022 10:47 a.m. Buenos días, para poder corregir ese error en el sistema operativo de la maquina virtual se necesita correr la herramienta CHKDSK y reiniciar el servidor. Quedamos atentos a la disponibilidad para poder realizar esa tarea, que puede tomar de unos minutos a una hora. 19/11/2022 9:21 p.m. Buenas noches, se procede a realizar el escaneo de disco, no se obtienen resultados adversos:Se procede a realizar la optimización de disco C: y se concluye exitosamente. No fue necesario el reinicio de la máquina virtual. Es de notar que si los cambios en el disco C: no superan los 8MB el proceso de defragmentación/optimización no va a correr y podría generar de nuevo un mensaje de error, pero eso es comportamiento esperado (si no hay nada que defragmentar no corre el proceso).	NO	0	100,00%
13-161122	Solicitud de servicio	16/11/2022	3:37 p.m.	Correo	Enlanube	Editar Regla en FW de DC agregar puertos	16/11/2022	3:45 p.m.	Juan Manuel Rojas	Se realiza la configuración solicitada en el firewall,	NO	0	100,00%
14-211122	Solicitud de servicio	21/11/2022	9:59 a.m.	Correo	Enlanube	acompañamiento FW y WAF 22/11/2022 hora 2pm	23/11/2022	10:41 a.m.	Juan Manuel Rojas	21/11/2022 11:01 a.m. Confirmo mi asistencia a la sesión en la fecha y hora programada, 23/11/2022 10:41 a.m. En sesión realizada el día de ayer, se ejecutó la configuración del servidor syslog con IP 192.168.60.44 (puerto 514) en los equipos Fortigate y Fortiweb de DC, procederán a realizar validaciones de funcionamiento e informar cualquier inconveniente que se llegue a presentar,	NO	0	100,00%
15-221122	Solicitud de servicio	22/11/2022	11:00 a.m.	Correo	Enlanube	VPN_ GLOBAL HITSS Agregar dominis y puertos	23/11/2022	11:56 a.m.	Juan Manuel Rojas	Se realiza la configuración solicitada en la vpn GLOBAL HITSS y las reglas 134/135:	NO	0	100,00%

16-221122	Solicitud de servicio	22/11/2022	2:44 p.m.	Correo	Enlanube	Eliminación y Aprovisionamiento VM APP	23/11/2022	12:23 p.m.	Javier Orejarena	23/11/2022 9:32 a.m. Buenos dias, estamos en proceso de aprovisionamiento, estaremos informando cuando esté lista la VM. 12:23 p.m. Buenas tardes, la máquina APLOG01 192.168.60.44 ha sido red desplegada con Debian 9.	NO	0	100,00%
17-231122	Solicitud de servicio	23/11/2022	2:12 p.m.	Correo	Enlanube	Regla Ip publica a 90.41	25/11/2022	10:04 a.m.	Juan Manuel Rojas	Se configura NAT en el firewall con la ip interna 192.168.90.41 y la ip publica 204.199.80.237 (puerto 80):	NO	0	100,00%
18-281122	Solicitud de servicio	28/11/2022	9:44 a.m.	Correo	Enlanube	Aprovisionamiento Maquina ASR-SRV04 - 192.168.40.33	29/11/2022	9:02 a.m.	Javier Orejarena	Buenos dias, ya se encuentra desplegada la máquina virtual ASR-SRV04 192.168.40.33 con los requerimientos solicitados por el cliente. Queda pendiente la integración al directorio activo, ésta la realiza el cliente. Quedamos atentos a cualquier novedad.	NO	0	100,00%
19-291122	Solicitud de servicio	29/11/2022	1:31 p.m.	Correo	Enlanube	Modificación regla FW 102	29/11/2022	3:56 p.m.	Juan Manuel Rojas	Se realiza la configuración solicitada en el firewall, quedando de la siguiente manera:	NO	0	100,00%
20-301122	Solicitud de servicio	30/11/2022	4:45 p.m.	Correo	Enlanube	VPN a AZAPTSE01	5/12/2022	11:21 a.m.	Juan Manuel Rojas	01/12/2022 9:22 a.m. En comunicación telefónica con el ingeniero Fabian Beltrán de ADRES, se programa sesión para el día de hoy a las 10:30 am, 05/12/2022 11:21 a.m. El día 01/12/2022 se realiza la configuración solicitada durante una sesión por teams realizada con los ingenieros Fabian y Wilmer de ADRES, quedando de la siguiente manera:	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 noviembre- 2022.

Contenido

1. DESCRIPCIÓN DEL SERVICIO	3
1.1. INFRAESTRUCTURA O DIAGRAMA DE LA SOLUCIÓN TECNOLÓGICA	3
2. ESPECIFICACIONES DEL SERVICIO CONTRATADO	0
2.1. DATA CENTER PRINCIPAL	0
2.1.1. SERVIDORES	0
2.1.2. ALMACENAMIENTO	3
3. DISPONIBILIDAD DEL SERVICIO	10
3.1. CONSUMO BACK UP	10
3.1.1. BACKUP DISCO REPOSITORIOS VEEAM	10
3.1.2. BACKUP A CINTA	11
3.2. CONSUMO DE COMPUTO (CPU Y RAM)	11
3.2.1. CLUSTER APLICACIONES	11
3.2.2. CLUSTER BASE DE DATOS	11
3.3. ESCANEEO DE SEGURIDAD	12
3.4. CASOS REPORTADOS	12
3.4.1. DISPONIBILIDAD ITX	13

1. DESCRIPCIÓN DEL SERVICIO

El servicio de Data Center brindado por **UT - INTERNEXA - ENLANUBE** para proveer los servicios solicitados por la **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		06 de diciembre 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**.

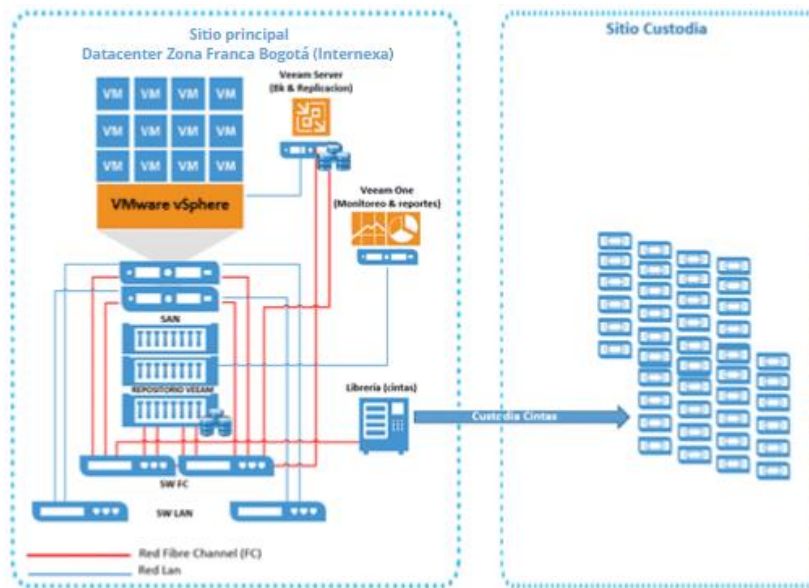


Figura 1. Infraestructura de la solución.

A continuación, se encuentra la topología actual.

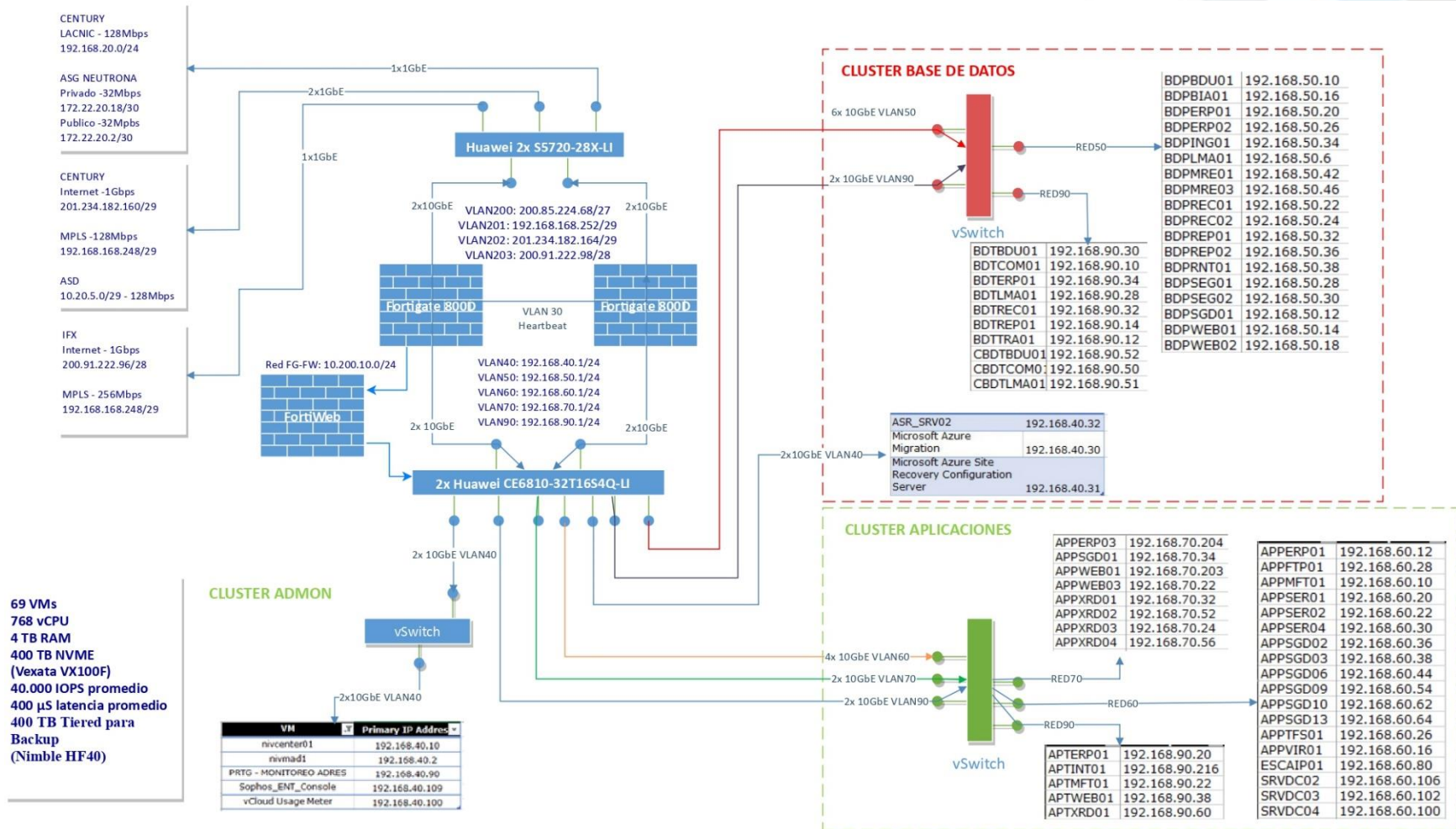


Figura 2. Topología actual

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 cómputo, conectividad, almacenamiento y gestión. A continuación, se explican uno a uno los servicios que conforman la infraestructura contratada por **INFRAESTRUCTURA 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.

DOCUMENTO TÉCNICO

Versión actual del documento 1.0

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	BDPRECO1	Microsoft Windows Server 2019	32	131	1	9	11.174
14	BDPRECO2	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.

DOCUMENTO TÉCNICO

Versión actual del documento 1.0

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 Estándar - 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 Estándar - 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 provisionados por **UT - INTERNEXA - ENLANUBE** contiene las características de cómputo de los servidores provisionados en ITX.

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

Total VM	VM NAME	OS according to the configuration file	vCPUs	Memory GB	NICs	Disk s	Provisioned GB
1	APPERP01	Microsoft Windows Server 2012 R2	16	32	2	5	810
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	2.704
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

DOCUMENTO TÉCNICO

Versión actual del documento 1.0

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	APTXR01	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	196
36	APTERP02	Microsoft Windows Server 2016	16	32	1	3	852
37	APTFAB01	Microsoft Windows Server 2019	16	32	1	3	426
			548	1383			

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).

DOCUMENTO TÉCNICO

Versión actual del documento 1.0

- **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	laaS 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	laaS 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.

Basic Information



Normal

The device is working well.

Device Model: Dorado5000 V3
 Device Location:
 Version: V300R002C10
 Patch Version: SPC100 SPH110
 SN: 2102351CMA10K8000003
 WWN: 21002c97b17d82ff
 SSD: 96
 Total Disk Capacity: 1.309 PB

Figura 3. Información de identificación del Almacenamiento provisionado.

Dentro del almacenamiento Huawei actualmente a nivel de producción se están consumiendo 622 TB

La tabla 12, Almacenamiento SAN Alto Rendimiento provisionado 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 provisionado por UT - INTERNEXA - ENLANUBE en ITX. SSD

Name	Type	# VMs	Provisioned MB
APDFAB01_0001	VMFS	2	853.714
APPMFT01_0001	VMFS	1	7.295.595
APPMFT01_0002	VMFS	1	6.243.391
APPMFT01_0003	VMFS	1	12.585.163

DOCUMENTO TÉCNICO
Versión actual del documento 1.0

APPSER01_0001	VMFS	2	4.802.879
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	9.668.252
APPSER02_0005	VMFS	1	7.342.280
APPSER04_0001	VMFS	2	15.098.631
APPSGD09_0001	VMFS	1	12.616.957
APPSGD09_0002	VMFS	1	11.608.164
APPSGD09_0003	VMFS	1	4.932.678
APPSGD10_0001	VMFS	1	7.722.263
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	2.426.183
APPVIR01_0001	VMFS	1	8.389.696
APPVIR01_0002	VMFS	1	8.389.688
APPVIR01_0003	VMFS	1	8.140.398
ASR_0001	VMFS	3	4.148.012
ASR_0002	VMFS	1	1.252.498
BDDFAB01_0001	VMFS	1	3.871.538
BDPBIA01N_0001	VMFS	1	953.007
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	132.423
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	3.115.219
BDPCOM01N_0015	VMFS	1	4.195.311
BDPCOM01N_0016	VMFS	1	3.146.729
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	329.544
BDPERP01N_0002	VMFS	1	296.364
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

DOCUMENTO TÉCNICO
Versión actual del documento 1.0

BDPERP01N_0007	VMFS	1	2.622.974
BDPERP02_0001	VMFS	1	3.245.943
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	11.004.297
BDPMRE01_0002	VMFS	1	12.592.871
BDPMRE02_0001	VMFS	1	11.284.164
BDPMRE02_0002	VMFS	1	12.374.283
BDPMRE02_0003	VMFS	1	2.098.651
BDPMRE03_0002	VMFS	1	8.472.668
BDPMRE03N_0001	VMFS	1	2.501.324
BDPMRE03N_0002	VMFS	1	4.195.953
BDPMRE03N_0003	VMFS	1	4.195.837
BDPMRE03N_0004	VMFS	0	1.524
BDPMRE03N_0005	VMFS	0	1.524
BDPMRE03N_0006	VMFS	1	2.000.056
BDPREC01_0001	VMFS	2	1.721.678
BDPREC01N_0001	VMFS	1	1.738.479
BDPREC01N_0002	VMFS	1	2.098.651
BDPREC01N_0003	VMFS	1	2.098.651
BDPREC01N_0004	VMFS	1	2.098.651
BDPREC01N_0005	VMFS	1	2.098.658
BDPREC01N_0006	VMFS	1	1.050.058
BDPREC02N_0001	VMFS	1	689.783
BDPREC02N_0002	VMFS	1	1.050.058
BDPREC02N_0003	VMFS	1	1.050.059
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	11.220.640
BDPWEB02_0001	VMFS	2	16.846.581
BDTERP01_0001	VMFS	1	7.285.139
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
BDTTA01N_0001	VMFS	1	14.133.858

DOCUMENTO TÉCNICO
Versión actual del documento 1.0

CBDTBDU01_0001	VMFS	1	7.406.969
CBDTCOM01_0001	VMFS	1	657.033
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	2.098.652
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	8.914.286
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	24	32.627.338
DS_APPS_0002	VMFS	5	13.232.285
DS_BD_0001	VMFS	12	7.579.850
DS_BD_0003	VMFS	2	5.571.117
DS_BD_0004	VMFS	1	8.701.125
DS_HUAWEI_ADMON	VMFS	11	4.057.185
UBDPBDU01_0001	VMFS	1	1.908.462
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	1.050.196
UBDPBDU01_0012	VMFS	1	1.050.059
UBDPBDU02_0001	VMFS	1	1.908.051
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

DOCUMENTO TÉCNICO
Versión actual del documento 1.0

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	832.205
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	2.098.591
UBDPLMA01_0011	VMFS	1	2.098.651
UBDPLMA02_0001	VMFS	1	832.203
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
			622.027.255

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
<input checked="" type="checkbox"/> BDPCOM02_0001	Normal	Online	Internal	2.000 TB	POOL01	Mapped	1.673 TB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0002	Normal	Online	Internal	2.000 TB	POOL01	Mapped	18.475 GB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0003	Normal	Online	Internal	2.000 TB	POOL01	Mapped	21.217 GB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0004	Normal	Online	Internal	2.000 TB	POOL01	Mapped	26.913 GB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0005	Normal	Online	Internal	2.000 TB	POOL01	Mapped	66.795 GB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0006	Normal	Online	Internal	2.000 TB	POOL01	Mapped	336.288 GB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0007	Normal	Online	Internal	2.000 TB	POOL01	Mapped	1.458 TB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0008	Normal	Online	Internal	2.000 TB	POOL01	Mapped	546.964 GB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0009	Normal	Online	Internal	2.000 TB	POOL01	Mapped	1.539 TB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0010	Normal	Online	Internal	2.000 TB	POOL01	Mapped	448.008 GB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0011	Normal	Online	Internal	2.000 TB	POOL01	Mapped	75.273 MB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0012	Normal	Online	Internal	2.000 TB	POOL01	Mapped	64.468 MB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0013	Normal	Online	Internal	2.000 TB	POOL01	Mapped	79.226 MB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0014	Normal	Online	Internal	2.000 TB	POOL01	Mapped	31.761 GB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0015	Normal	Online	Internal	4.000 TB	POOL01	Mapped	3.709 TB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0016	Normal	Online	Internal	3.000 TB	POOL01	Mapped	2.794 TB	SQL_Server_OLAP&OLTP
<input type="checkbox"/> BDPCOM02_0017	Normal	Online	Internal	2.000 TB	POOL01	Mapped	0.000 MB	SQL_Server_OLAP&OLTP

DOCUMENTO TÉCNICO
Versión actual del documento 1.0

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.

DOCUMENTO TÉCNICO
Versión actual del documento 1.0

<input type="checkbox"/>	Name	Health Status	Running Status	Capacity	Owning Storage Pool
<input type="checkbox"/>	BACKUP0001	Normal	Online	128.000 TB	POOL01
<input type="checkbox"/>	BACKUP0002	Normal	Online	128.000 TB	POOL01
<input type="checkbox"/>	BACKUP0003	Normal	Online	128.000 TB	POOL01
<input type="checkbox"/>	BACKUP0004	Normal	Online	128.000 TB	POOL01
<input type="checkbox"/>	BACKUP0005	Normal	Online	256.000 TB	POOL01

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

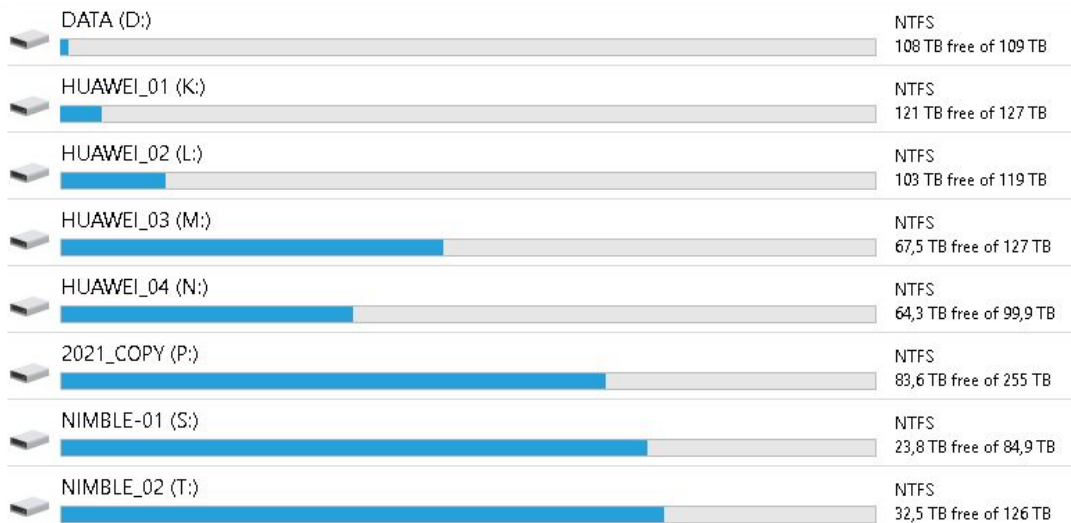
3. DISPONIBILIDAD DEL SERVICIO

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 444,1 TB), políticas diarias y semanales.

Figura 5. Consumo de back up Repositorios Veeam



Repositorio	Tamaño uso [TB]
DATA	1
HUAWEI_01	6
HUAWEI_02	16
HUAWEI_03	59,5
HUAWEI_04	35,6

DOCUMENTO TÉCNICO
Versión actual del documento 1.0

2021_COPY	171,4
NIMBLE_01	61,1
NIMBLE_02	93,5
TOTAL	444,1

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 noviembre 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 noviembre 2022.

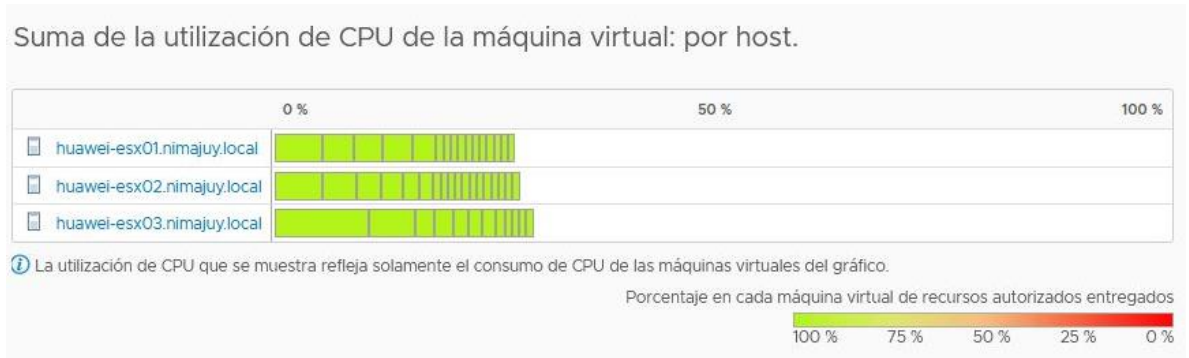


Figura 6. Consumo de CPU en Cluster de Aplicaciones

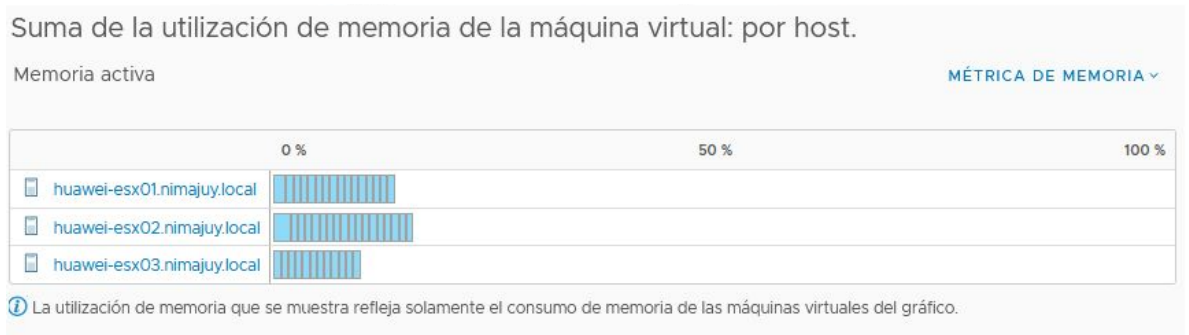


Figura 7. Consumo de memoria en Cluster de Aplicaciones.

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 noviembre 2022.

DOCUMENTO TÉCNICO

Versión actual del documento 1.0

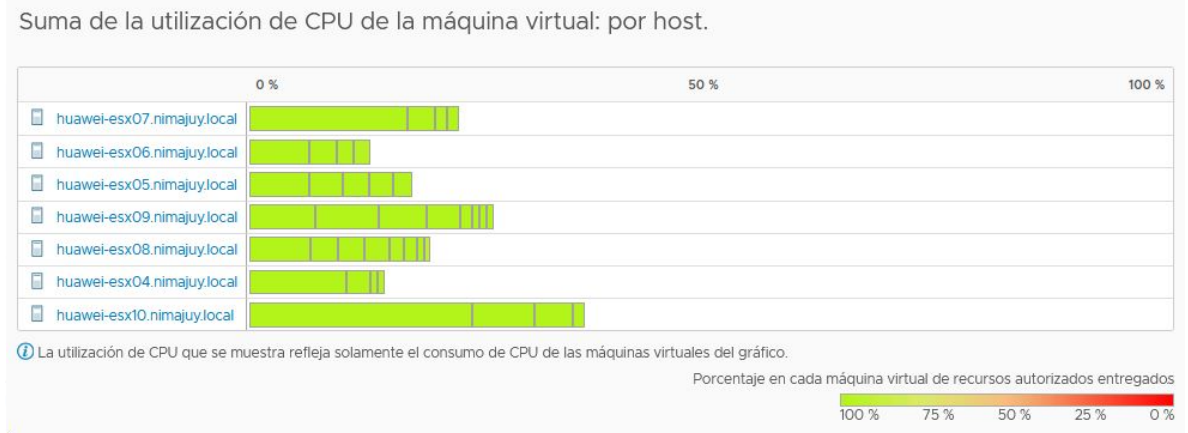


Figura 8. Consumo CPU en el Cluster de Base de datos.

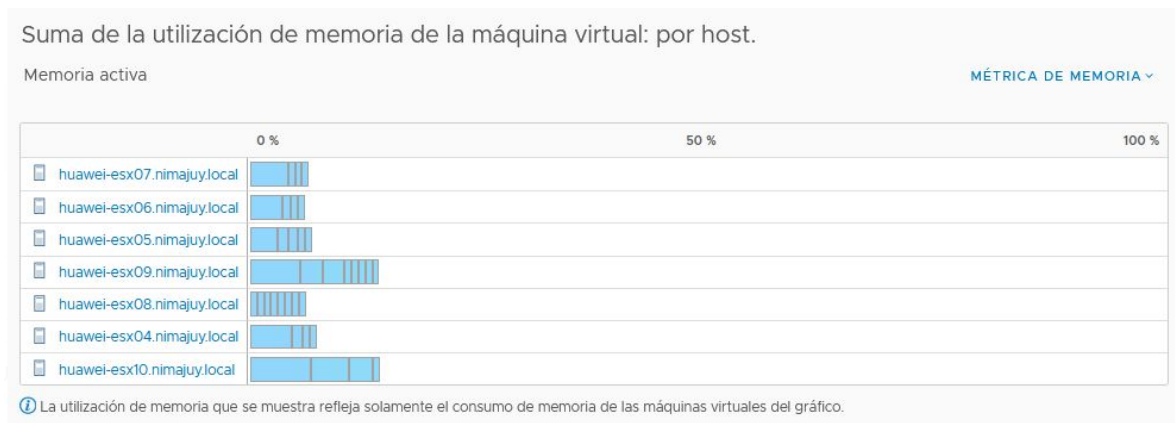


Figura 9. Consumo de Memoria en el Cluster de Base de datos.

3.3. ESCANEOS 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 noviembre y su clasificación.

Tabla 16. Casos registrados en el mes de noviembre 2022. Se envía en archivo anexo 4.

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

DOCUMENTO TÉCNICO
Versión actual del documento 1.0

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

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 noviembre 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 NOVIEMBRE DE 2022

The enlanube logo, consisting of a stylized orange and blue shape followed by the text "enlanube" in a sans-serif font.

Soporte EnLaNube

soporte@enlanube.com.co

monitoreo.cliente@enlanube.com.co

Tel: 5085603 – 018005184539

CONTENIDO

1.	OBJETIVO	3
2.	DESARROLLO.....	3
3.	DEFINICIONES	3
4.	DISPONIBILIDAD DE RECURSOS	5
4.0	Disponibilidad Plataforma.....	5
4.1	Dispositivos integrados por protocolo	6
4.2	Dispositivos por tiempo de disponibilidad.....	6
5.	USO DE COMPONENTES	7
5.0	Uso de licenciamiento	7
5.1	Dispositivos por tasa de evento	7
6.	RENDIMIENTO	8
6.0	CPU	8
6.1	MEMORIA	8
7.	EVENTOS RELEVANTES.....	9
7.0	Top de IPs con Malware.....	9
7.1	Trafico de salida permitido por destino	10
7.2	Top de Fuentes con más conteos de Bloqueos.....	10
7.3	Firewall Deny: Top de Destinos con más conteos de denegaciones.....	10
7.4	Firewall: Top de cambios realizados	11
8.	INCIDENTES.....	11
8.0	Vista Global.....	11
8.1	Incidentes de Disponibilidad.....	12
8.2	Incidentes de rendimiento.....	14
8.3	Incidentes de seguridad severidad alta.....	15
9.	ACTIVIDADES ADICIONALES RELEVANTES DEL MES.....	18
10.	ACCIONES DE MEJORA.....	18
11.	CONCLUSIONES.....	18

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 públicas fuera de Colombia.

- **Mirai.Botnet**

Mirai es un malware de la familia de los 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 28 días y el equipo Servidor en un tiempo de operación desde los últimos 41 días, los cuales están en estado Warning, ya que al momento de la captura el SIEM está realizando una actualización de componentes.

INFORME ADRES

Name	IP Address	Module Role	Health	Last Status Updated
ELNF55.ENLANUBE.COM.CO	10.99.93.120	Super	Warning	Dec 01 2022, 02:41:22 PM

Owner	Status	Uptime
admin	up	41d 2h

Organization	Name	IP Address	Health	Uptime	Collector ID
Adres	CollectorAdres	10.90.54.10	Warning	28d 1h	10001

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 Noviembre del 2022.

Los servidores Windows no están reportando por WMI, se realizó la actualización del colector para retomar la instalación y configuración del protocolo WMI en los dispositivos.

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 Noviembre 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 presente una alta indisponibilidad por lo cual se cuenta con un SLA de 100%.

<input checked="" type="checkbox"/>	Host Name	Current Uptime	Total Downtime	Achieved Uptime (SLA)
<input checked="" type="checkbox"/>	APPWEB01.adres.gov.co	20d 4h	11s	100
<input checked="" type="checkbox"/>	APPINT01.adres.gov.co	20d 4h	11s	100

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

5. USO DE COMPONENTES

5.0 Uso de licenciamiento

Del licenciamiento habilitado para el cliente ADRES de una tasa de eventos mínima de 7,37 EPS y un máximo de hasta 500 EPS, en promedio diariamente se están utilizando 117 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	FINS	Not Specified	0

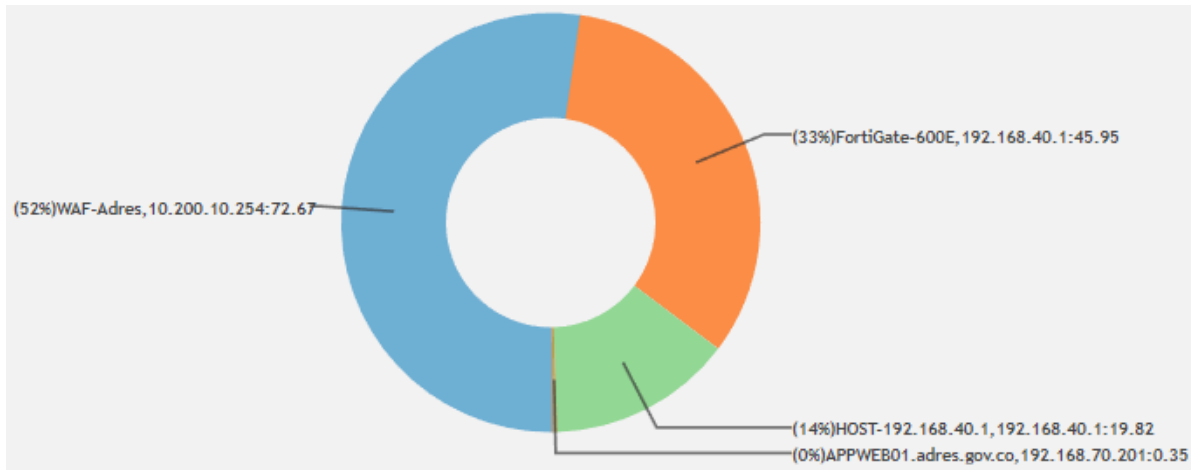
Rank	Organization ID	Reporting IP	AVG(Event Rate)	MAX(Event Rate)	MIN(Event Rate)
1	2001	10.90.54.10	117.28	500.37	7.37

Ilustración 4 Uso de licenciamiento durante el mes de Noviembre 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 Fortissem.

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.



INFORME ADRES

<input checked="" type="checkbox"/> Reporting Device	Reporting IP	AVG(Event Rate)
<input checked="" type="checkbox"/> WAF-Adres	10.200.10.254	72.67
<input checked="" type="checkbox"/> FortiGate-600E	192.168.40.1	45.95
<input checked="" type="checkbox"/> HOST-192.168.40.1	192.168.40.1	19.82
<input checked="" type="checkbox"/> APPWEB01.adres.gov.co	 192.168.70.201	0.35
<input checked="" type="checkbox"/> APPINT01.adres.gov.co	 192.168.60.2	0.28

Ilustración 5 Tasa de eventos por dispositivos durante el mes de Noviembre 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:



<input checked="" type="checkbox"/> Host Name	Host IP	AVG(CPU Util)	MAX(CPU Util)	MIN(CPU Util)
<input checked="" type="checkbox"/> APPWEB01.adres.gov.co	 192.168.70.201	7.25%	44.44%	0.44%
<input checked="" type="checkbox"/> APPINT01.adres.gov.co	 192.168.60.2	1.63%	23.12%	0.00%

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

Se verifica que los dispositivos no cuentan con consumos críticos de CPU en promedio, se evidencian caídas fuertes de CPU y un uso eventual de hasta el 44% 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:

<input checked="" type="checkbox"/> Host Name	AVG(Memory Util)	MAX(Memory Util)	MIN(Memory Util)
<input checked="" type="checkbox"/> APPINT01.adres.gov.co	33.70%	54.87%	4.87%
<input checked="" type="checkbox"/> APPWEB01.adres.gov.co	31.14%	61.90%	3.69%

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

Se verifica que los dispositivos cuentan con un consumo promedio estable, pero se han presentado consumos altos de un 61% 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 e IPS:

Destination IP	Event Name	COUNT
66.240.205.34	Bladabindi.Botnet	19
66.240.205.34	Gh0st.Rat.Botnet	17
106.75.3.35	Ganiw.Botnet	16
106.75.3.35	Gh0st.Rat.Botnet	13
194.55.186.97	Mirai.Botnet	11
106.75.3.35	Bladabindi.Botnet	9
106.75.173.138	RotaJakiro.botnet	4
109.206.243.17	Mirai.Botnet	4
185.216.71.17	Mirai.Botnet	4
1.246.222.13	Mirai.Botnet	1

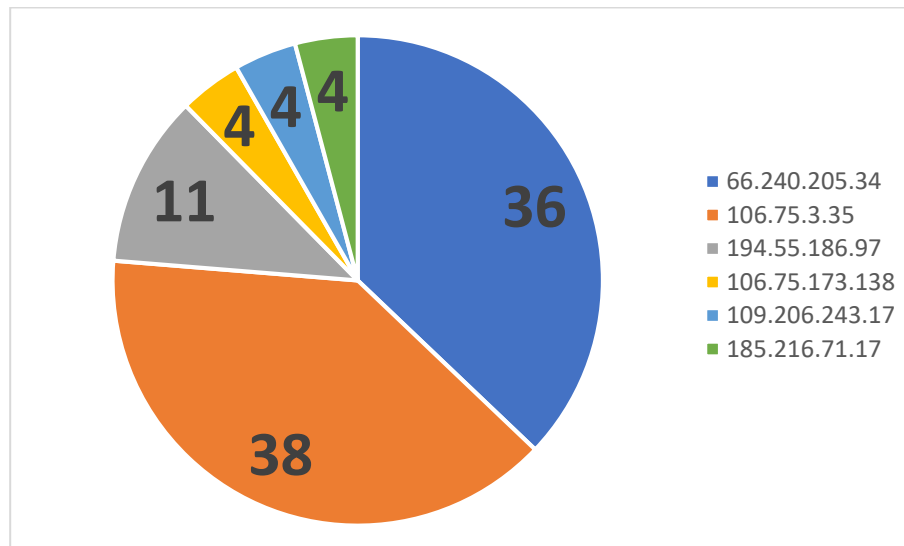


Ilustración 8 Top de IPs con malware reportados durante el mes de Noviembre 2022

Se sugiere realizar una validación con el administrador de la red ya que las IPs reportadas son públicas, con varias firmas de Malware detectadas.

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:

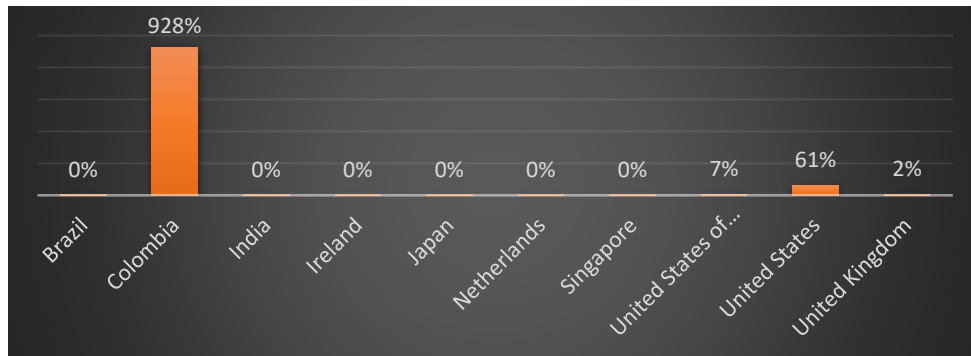


Ilustración 9 Top países de tráfico permitido durante el mes de Noviembre 2022

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:

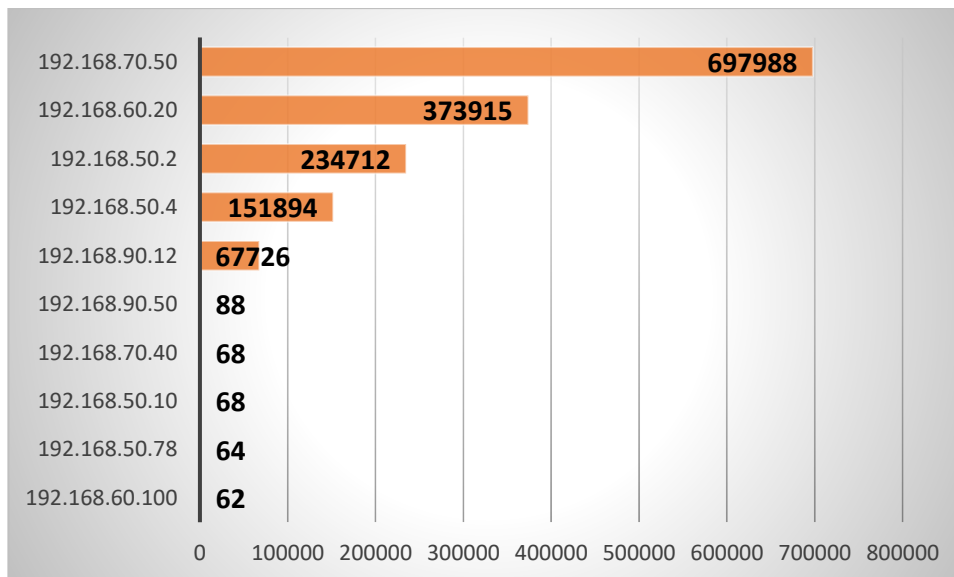


Ilustración 10 Top fuentes con más bloqueos reportados durante el mes de Noviembre 2022

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:

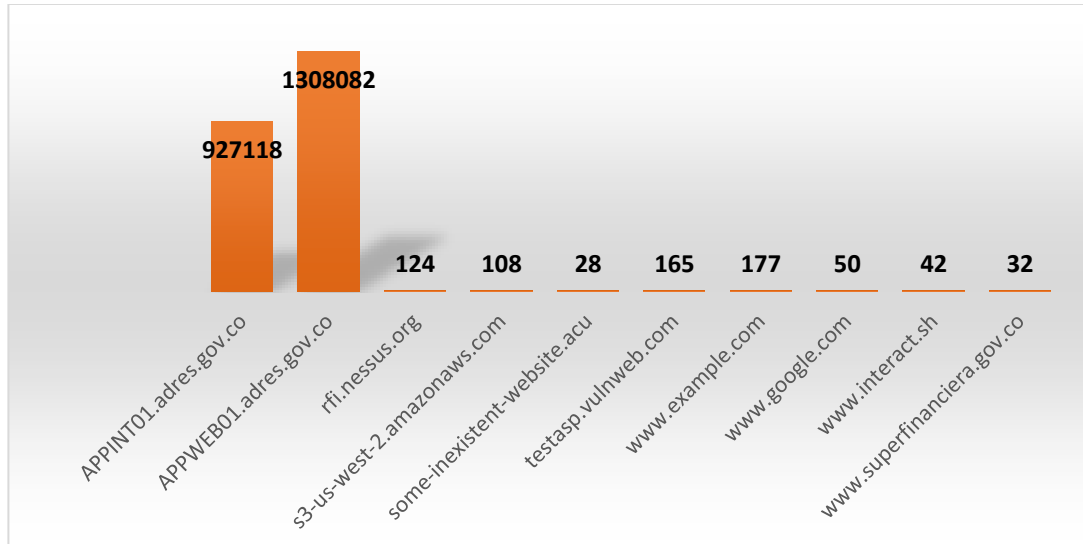


Ilustración 11 Top de categorías con más bloqueos reportados durante el mes de Noviembre 2022

En la siguiente imagen podremos encontrar las categorías y páginas visitadas más relevantes, en donde observamos que el mayor destino fueron los server APPINT01 y APPWEB01, también se evidencian destinos propios del dominio Nessus perteneciente a una solución de ciberseguridad y análisis de vulnerabilidades.

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	frojasv	No usuario	adresvisor	Total general
Add	92,98%	7,02%	0,00%	0,00%	100,00%
Delete	100,00%	0,00%	0,00%	0,00%	100,00%
Edit	73,08%	23,08%	0,00%	3,85%	100,00%
Move	100,00%	0,00%	0,00%	0,00%	100,00%
update	0,00%	0,00%	100,00%	0,00%	100,00%
Total general	18,00%	2,22%	79,56%	0,22%	100,00%

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

Se puede observar que el 79% de los cambios realizados son por actualización, seguido por el 18% de cambios realizados por el usuario admin y un 2,22% de cambios realizados por el usuario frojasv, se recomienda validar los cambios a nivel de eliminación y traspaso.

8. INCIDENTES

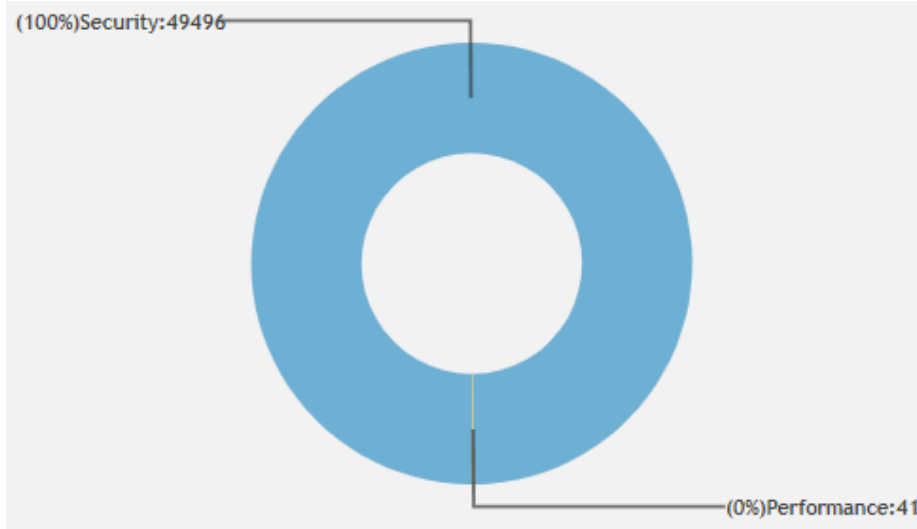
8.0 Vista Global

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 performance con el 0 %.



<input checked="" type="checkbox"/> Incident Category	Count
<input checked="" type="checkbox"/> Security	49,496
<input checked="" type="checkbox"/> Performance	41
<input checked="" type="checkbox"/> Availability	37
<input checked="" type="checkbox"/> Change	5

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

INFORME ADRES

<input checked="" type="checkbox"/> Event Name	Event Severity	Severity Category	Count
<input checked="" type="checkbox"/> Missing specific performance metric from a device	10	HIGH	17
<input checked="" type="checkbox"/> Server Down: No Ping Response	10	HIGH	9
<input checked="" type="checkbox"/> System Collector Event Delayed	9	HIGH	1
<input checked="" type="checkbox"/> Sudden Decrease in Reported Events From A Host	7	MEDIUM	7
<input checked="" type="checkbox"/> No logs from a device	7	MEDIUM	3

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

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

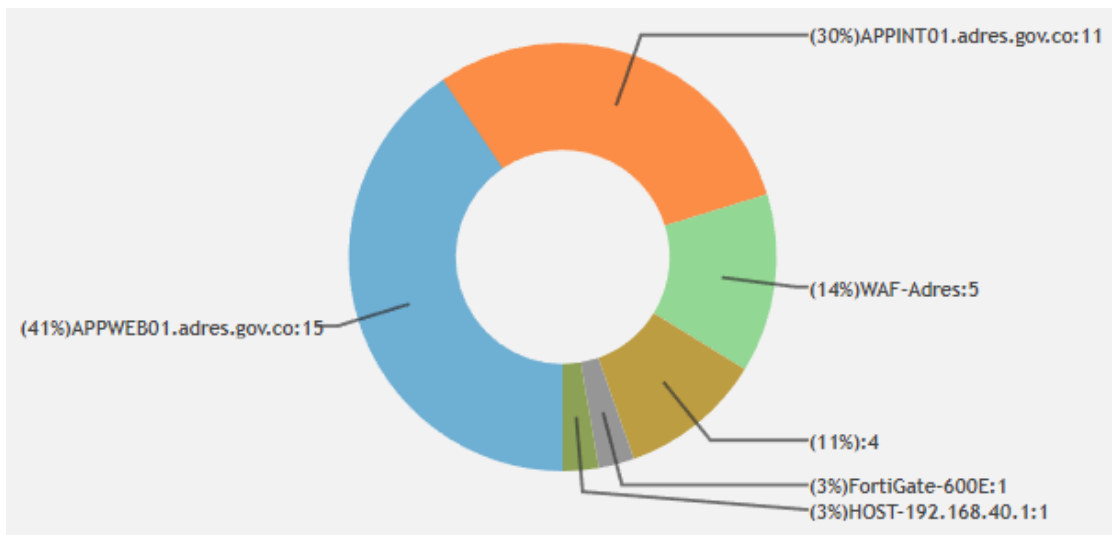


Ilustración 15 Top incidentes de indisponibilidad por dispositivo durante el mes de Noviembre 2022.

Se puede observar que el dispositivo con mayor conteo de incidentes de disponibilidad es el dispositivo APPIWEB01 con 15 eventos, seguido del dispositivo APPINT01 con 11 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.

<input checked="" type="checkbox"/> Missing specific performance metric from a device	10	HIGH	17
<input checked="" type="checkbox"/> Server Down: No Ping Response	10	HIGH	9

- **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, los que se presentaron fue durante un tiempo no mayor a 11 segundos para los dos servidores que lo reportaron, lo cual es por una pequeña falla en la comunicación, el incidente Missing Specific obedece a la misma razón.

- **System Collector Event Delayed**

Se detecta que el equipo collector no reporta data al SIEM por más de 10 minutos, esto sucedió iniciando el mes cuando fue necesario aplicar un reinicio sobre el equipo collector para que finalizara las actualizaciones, sin embargo la data es almacenada y luego de los 10 minutos se reporta al SIEM.

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 Noviembre 2022.

<input checked="" type="checkbox"/> Event Name	Event Severity	Severity Category	Count
<input checked="" type="checkbox"/> Sudden Increase in STM Response Times	7	MEDIUM	19
<input checked="" type="checkbox"/> Server Disk space Warning	5	MEDIUM	15
<input checked="" type="checkbox"/> Sudden Increase in SNMP Response Times	7	MEDIUM	6
<input checked="" type="checkbox"/> Server Disk Space Critical	9	HIGH	1

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

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

<input checked="" type="checkbox"/> Host Name	Count
<input checked="" type="checkbox"/> APPWEB01.adres.gov.co	24
<input checked="" type="checkbox"/> APPINT01.adres.gov.co	12
<input checked="" type="checkbox"/> HOST-138.91.123.30	5

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

Se puede observar que el dispositivo con mayor conteo de incidentes de rendimiento es el dispositivo APPWEB01 con 24 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 Noviembre 2022.

<input checked="" type="checkbox"/> Event Name	Event Severity	Severity Category	Count
<input checked="" type="checkbox"/> Blocklist User Agent Match	10	HIGH	2,549
<input checked="" type="checkbox"/> Log4J Exploit Request Detected on Network by Fortinet Products	10	HIGH	3
<input checked="" type="checkbox"/> Inappropriate Website access: High volume	9	HIGH	798
<input checked="" type="checkbox"/> Stealth Scan	9	HIGH	781
<input checked="" type="checkbox"/> Microsoft Exchange Autodiscover RCE Detected on Network	9	HIGH	317
<input type="checkbox"/> Permitted Traffic from FortiGuard Malware IP List	9	HIGH	316
<input type="checkbox"/> Backdoor Found	9	HIGH	5
<input type="checkbox"/> Apache Path Traversal Vuln Detected on Network	9	HIGH	2
<input type="checkbox"/> Multiple Distinct IPS Events From Same Src	9	HIGH	2
<input type="checkbox"/> Concurrent VPN Authentications To Same Account From Different Cities	9	HIGH	1
<input type="checkbox"/> Sudden User Location Change	9	HIGH	1

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

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

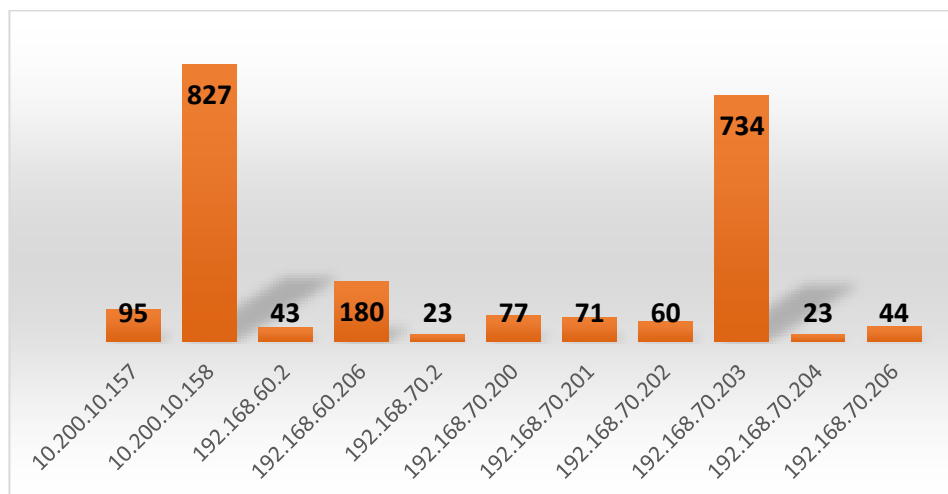


Ilustración 19 Top incidentes de seguridad por dispositivo durante el mes de Noviembre 2022.

INFORME ADRES

Se puede observar que el dispositivo con mayor conteo de incidentes de seguridad es el dispositivo con IP 10.200.10.158, con 827 eventos, seguido del dispositivo 192.168.70.203 con 734 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, para **inappropriate 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 984 ataques de los cuales se permitieron 98.

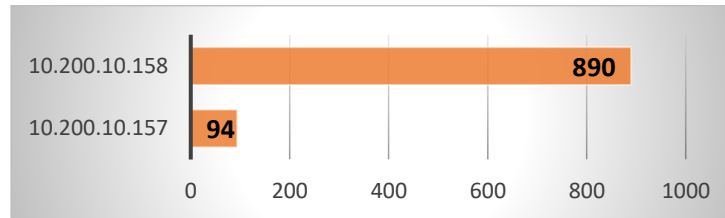


Ilustración 20 Top incidentes de Stealth Scan por dispositivo durante el mes de Noviembre 2022.

Evento	Deny	Permit	Total
Cisco.Smart.Install.Feature.Enable.Scanner		4	4
Nmap.Script.Scanner	98	1	99
ZGrab.Scanner	741	92	833
Muieblackcat.Scanner	2		2
Masscan.Scanner	40	1	41
Nessus.Scanner	2		2
ZmEu.Vulnerability.Scanner	3		3
Total	886	98	984

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

- **Blocklist User Agent Match:** Este incidente se genera luego de detectar una coincidencia con la lista de agentes de usuario http bloqueados. Malware, Adware, Spyware, etc. utilizan agentes de usuario poco comunes.

HTTP User Agent	Cuenta
Java/1.8.0_322	1069
libwww-perl/6.61	7
Wget/1.15 (linux-gnu)	29
Total general	1105

Ilustración 22 Top incidentes de Blocklist User Agent Match por firmas durante el mes de Noviembre 2022.

INFORME ADRES

Para este caso el agente reportado con mayor regularidad es: HTTP User Agent: Java/1.8.0_322 y el destino IP con mayor reporte es 192.168.70.203 y HTTP Host **aplicaciones.adres.gov.co**, por lo cual se sugiere validar si este agente corresponde a algún servicio permitido ya que se reporta hacia la misma dirección y por el mismo agente.

Destino IP	Cuenta
192.168.70.200	9
192.168.70.201	11
192.168.70.203	1081
Total general	1101

- **Log4J Exploit Request Detected on Network by Fortinet Products:** Solicitud de explotación de Log4J detectada en la red por un producto de Fortinet ó vista por un producto de Fortinet, en la cual se puede observar el dispositivo que lo reporto, desde donde se generó el incidente y el destino IP, todas las acciones fueron dropeadas por el Firewall.




Event Receive Time	Reporting Device	Source IP	Destination IP	Firewall Action	Event Name
Nov 19 2022, 07:21:22 PM	FortiGate-600E	 167.99.144.251	10.200.10.158	dropped	Apache.Log4j.Error.Log.Remote.Code.Execution
Nov 13 2022, 09:37:19 PM	FortiGate-600E	 159.223.199.108	10.200.10.158	dropped	Apache.Log4j.Error.Log.Remote.Code.Execution
Nov 13 2022, 09:01:56 PM	FortiGate-600E	 159.223.199.108	10.200.10.158	dropped	Apache.Log4j.Error.Log.Remote.Code.Execution
Nov 05 2022, 10:00:10 AM	FortiGate-600E	 165.232.155.171	10.200.10.158	dropped	Apache.Log4j.Error.Log.Remote.Code.Execution

Ilustración 23 Top incidentes de Log4J Exploit Match por firmas durante el mes de Noviembre 2022.

- **Microsoft Exchange Autodiscover RCE ProxyNotShell Detected on Network:** Este incidente se genera luego de que el WAF nos reporta tráfico que están relacionado con las vulnerabilidades (CVE-2022-41040, CVE-2022-41082), en base a ello se realizó la validación en la base de datos y no es un incidente que como tal tenga una mitigación, sino que más bien se sugiere desde las vulnerabilidades detectadas dos cosas.

a. Realizar un scan de vulnerabilidades a los dispositivos reportados o la infraestructura que se requiera necesaria, que en este caso son:

192.168.70.206, 192.168.70.203, 192.168.70.204, 192.168.60.2, 192.168.60.216, 192.168.60.206, 192.168.70.200, 192.168.70.203, 192.168.70.201

b. Validar los servidores que contengan servicios de microsoft Exchange en ejecución y aplicar los parches de seguridad sugeridos en los siguientes enlaces proporcionados de acuerdo a las vulnerabilidades detectadas

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040>

Para los demás incidentes reportados, hacen parte propiamente del incidente reportado SCAN, ya que obedecen a firmas y tipo de escaneo, los cuales se reportan como denegados y los permitidos en la tabla del punto **Stealth Scan**.

9. ACTIVIDADES ADICIONALES RELEVANTES DEL MES

Los cambios reportados obedecen a la actualización del equipo collector, el cual se deja en la última versión disponible y que opera de manera conjunta con la versión del supervisor, sin ninguna novedad.

10. ACCIONES DE MEJORA

Configuración de los protocolos SNMPv3 en el dispositivo AdresFSCo, FortiGate-600E y WAF-Adres, para recopilar información complementaria 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 y las IPs públicas reportadas, ya que son las que genera mayor reporte de eventos.
3. Se sugiere realizar un scan de vulnerabilidades hacia la infraestructura a fin de revisar los diferentes puertos y servicios utilizados, ya que se están generando incidentes anteriormente reportados con dichas condiciones.