



F-GC-29
Versión 1
Octubre 2016

EMPOCALDAS S.A E.S.P
GESTIÓN DE CONTRATACIÓN

LISTA CHEQUEO PAGO DE ACTAS - CONTRATOS PRESTACIÓN DE
SERVICIOS Y CONSULTORIA

# CONTRATO Y AÑO	0089/2019	Acta N°	1 Y FINAL	1. VALOR INICIAL (incluido IVA)	127,115,071
				2. VALOR ADICION (+)	0
CONTRATISTA	DATA & SERVICE LTDA			3. VALOR TOTAL (1+2)	127,115,071
NIT O CC:	810001025-7			4. VALOR ACTAS ANTERIORES (-)	0
CDP (#, rubro y fecha)	0266 DE 28 DE ENERO DE 2019			5. VALOR PRESENTE ACTA (-)	127,115,071
RP (#, rubro y fecha)	0278 DEL 08 DE FEBRERO DE 2019			6. VALOR NO EJECUTADO	0

OBJETO DEL CONTRATO: FORTALECIMIENTO DEL SISTEMA DE PROTECCIÓN CONTRA ATAQUES INFORMATICOS A LA EMPRESA.

TIPO DE RECURSOS	PROPIOS	CENTRO DE COSTOS y PROCEDIMIENTO
------------------	---------	--

DOCUMENTO VERIFICADOS		# FOLIOS
1- Autoliquidaciones en Salud, Pensiones y Riesgos profesionales del personal empleado y del contratista (Personas naturales) o Certificado de Cumplimiento del Artículo 50 de la Ley 789/02 (Personas jurídicas).	X	
2- Factura (Régimen Común) o Factura equivalente (régimen simplificado).	X	
3- Pagos SENA y ICBF.		
4- Evaluación del Supervisor Formato F-CG-18 (Solo aplica para el acta final)	X	
5- Planillas de pago con firma de los trabajadores (cuando se cuente con personal a cargo).		
6- Informe de actividades a cargo del Supervisor.	X	

Nota: Si pasados tres (3) días después del recibo de esta documentación el Supervisor del contrato no presenta correcciones, quedará en firme y será subida al SECOP.

Secretaría General CERTIFICA que el Supervisor del Contrato entregó la documentación para ser archivada en la carpeta correspondiente.

Edna Suarez A
NOMBRE DE QUIEN RECIBE

[Firma] 02-04-2019
FIRMA

DOCUMENTOS ANEXOS CON DESTINO A TESORERÍA	
Factura (Régimen Común) o Factura equivalente (régimen simplificado).	X
Evaluación del Supervisor F-CG-18 (Solo aplica para el acta final).	X
Informe de actividades a cargo del Supervisor.	X
Copia del Registro Presupuestal.	X
Autoliquidaciones en Salud, Pensiones y Riesgos profesionales del personal empleado y del contratista (Personas naturales) o Certificado de Cumplimiento del Artículo 50 de la Ley 789/02 (Personas jurídicas).	X
Distribución por centro de costos. Formato F-GF-32	

Fecha de presentación 22 DE MARZO DE 2019

DATOS DEL SUPERVISOR	
JOHN JAIRO GIRALDO VILLA	JEFE SECCION SISTEMAS
NOMBRE	CARGO
	FIRMA

DATOS PARA LA TRANSFERENCIA DE PAGOS		
07087610611	AHORROS	BANCOLOMBIA
CUENTA	TIPO DE CUENTA	BANCO

PBX 8812277

www.datayservice.com

Manizales

Data & Service

"Un Servidor en Quien Confiar"



data & service
NIT. 810001025-7

FACTURA DE VENTA No.:

12241

CALLE 54 No. 26-60

FECHA: 2019/03/21

MANIZALES

NIT: 810.001.025-7

Presente su factura
Para hacer efectiva
su garantía.

TEL: 8812277

IVA REGIMEN COMÚN

Informacion@datayservice.com

Información del Cliente:

NOMBRE : EMPOCALDAS S.A. E.S.P

NIT/CC : 890803239

DIRECCION: CRA. 23 NRO. 75-82

TEL/FAX: 8867080

CIUDAD : MANIZALES

VENDEDOR : 00

VENCE : 2019 04 21

UNIDADES	DESCRIPCION	VALOR UNITARIO	VALOR NETO
1	SOFT. CISCO ANYCONNECT PLUS LI	2,628,800.00	2,628,800.00
1	CISCO SVP UMBRELLA INSIGHTS	55,410,411.00	55,410,411.00
1	SOFT. SVP CISCO ADVANCED MALWA	22,586,712.00	22,586,712.00
1	SOFT. CISCO PROTECCIÓN SEGURID	45,989,676.00	45,989,676.00
1	TRAFICO EMAIL CORREO ENTRANTE	0.00	0.00

AUTORIZACION DE FACTURACION FORMULARIO No 18762007670535 DEL 06/04/2018 HABILITACION DEL 12083 AL 18000 VIGENCIA 24 MESES

Observaciones

Recibido

DATA & SERVICE LTDA
NIT: 810.001.025-7
Tel: 8812277

[Firma]

CONTRATO No. 0089-2019

SUBTOTAL \$ 126,615,599

DESCUENTO \$ 0.00

IVA \$ 499,472.00

TOTAL \$ 127,115,071

FIRMA Y SELLO ALMACÉN

Firma Documento o Sello


Esta factura se asimila en todos sus efectos a una letra de cambio según el artículo 774 del código de comercio. Causara intereses por la mora a la máxima tasa permitida después de su vencimiento, según el artículo 884 del código de comercio.

**CERTIFICACION ACREDITACION PAGO DE APORTES DE SEGURIDAD SOCIAL Y
PARAFISCALES**

Yo, FERNANDO BETANCOURT ESCOBAR, identificado con cédula ciudadanía No. 10.278.051, en mi condición de Representante Legal de DATA Y SERVICE LTDA. Identificada con NIT. 810.001.025-7, debidamente inscrito en la Cámara de Comercio de Manizales certifico el pago de los aportes realizados por la compañía durante los últimos seis (6) meses por los conceptos de salud, pensiones, riesgos profesionales, cajas de compensación familiar, Instituto Colombiano de Bienestar familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA).

Lo anterior, en cumplimiento de lo dispuesto en el artículo 50 de la Ley 789 de 2002.

Dada en Manizales a los veintiún (21) días del mes de marzo (03) del año dos mil diecinueve (2019).



FERNANDO BETANCOURT ESCOBAR
C.C. 10.278.051

ACTA DE RECIBO # 1 Y FINAL

CONTRATO No. 0089/2019

OBJETO FORTALECIMIENTO DEL SISTEMA DE PROTECCION CONTRA ATAQUES INFORMATICOS A LA EMPRESA EMPOCALDAS S.A E.S.P

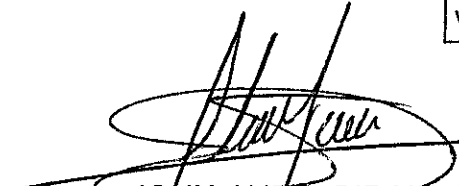
CONTRATISTA DATA & SERVICE LTDA

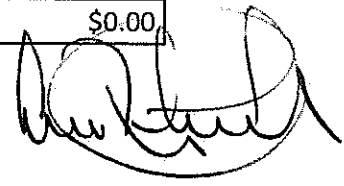
VALOR CONTRATO \$127.115.071

RECURSOS PROPIOS

En la ciudad de Manizales a los veintiún (21) días del mes de marzo de 2019, se reunieron JOHN JAIRO GIRALDO VILLA, Jefe de la Sección de Sistemas de EMPOCALDAS S.A E.S.P, en representación de la Empresa Contratante y FERNANDO BETANCOURT ESCOBAR, Representante Legal de la Empresa DATA & SERVICE LTDA, como contratista, con el fin de realizar el Acta de Recibo No. 1 y final al Contrato No. 0089 de 2019.

VALOR CONTRATO	\$127,115,071.00
ACTA # 1	\$127,115,071.00
VALOR EJECUTADO	\$127,115,071.00
VALOR POR EJECUTAR	\$0.00,


JOHN JAIRO GIRALDO VILLA
Jefe Sección Sistemas
Empocaldas S.A E.S.P


FERNANDO BETANCOURT E.
Representante Legal
DATA & SERVICE LTDA.

INFORME DE SUPERVISION

CONTRATO	Nº 0089/2019
CONTRATISTA	DATA & SERVICE LTDA
OBJETO	FORTALECIMIENTO DEL SISTEMA DE PROTECCION CONTRA ATAQUES INFORMATCIOS A LA EMPRESA
VALOR	\$127.115.071
RECURSOS	PROPIOS

En cumplimiento del contrato 0089/2019, cuyo objeto es el FORTALECIMIENTO DEL SISTEMA DE PROTECCION CONTRA ATAQUES INFORMATICOS A LA EMPRESA EMPOCALDAS S.A E.S.P, se evidencia que dicho contrato se desarrolla satisfactoriamente a los términos y especificaciones del contrato según el objeto contractual mencionado, se evidenció que dicho contrato se desarrolló satisfactoriamente a los términos y especificaciones del contrato según el objeto contractual mencionado y cumple con los pagos por concepto de seguridad social y parafiscales, cumplen también con las afiliaciones a salud, pensiones, cesantías y riesgos profesionales.

Manizales, 21 de marzo de 2019



JOHN JAIRO GIRALDO VILLA
Jefe Sección Sistemas

Preparó: María del Carmen Guzman Quintero

**INFORME ENTREGA
MIGRACIÓN FIREWALL
EMPOCALDAS**

Contenido

1. DERECHOS DEL DOCUMENTO	3
2. OBJETIVO	3
3. DESARROLLO DEL PROYECTO	3
4. ARQUITECTURA DE RED	4
4.1. Arquitectura Previa	4
4.2. Arquitectura después de la migración	6
4.2.1. Integración con Directorio Activo	7
4.2.2. Reglas de Firewall.....	7
4.2.3. Licenciamiento Actual	18
4.2.4. Direccionamiento IP	19
4.2.5. Gestión y administración.....	20
4.2.6. Usuario Gestión.....	20

1. DERECHOS DEL DOCUMENTO

Documento de uso interno y exclusivo de la Empresa que contiene información confidencial de Empocaldas, por lo cual Data y Service LTDA se compromete a resguardar y utilizar la información contenida en el mismo para los fines pertinentes y a respetar los acuerdos de confidencialidad establecidos y firmados entre las partes. Así mismo, este documento se considera propiedad de Data y Service y su divulgación parcial o total a terceros, no está permitida sin el consentimiento previo y explícito de la Empresa.

2. OBJETIVO

Establecer y explicar la ingeniería de detalle realizada durante la ejecución de las actividades de migración del firewall que provee la seguridad perimetral a Empocaldas. Esta contempla la instalación y configuración de los equipos Cisco FTD, con base al diseño propuesto en el plan de pre-venta e implementación previamente aprobado por Empocaldas.

3. DESARROLLO DEL PROYECTO

A continuación, se encuentra la lista de actividades realizadas durante el proceso de implementación y migración del firewall, el cual suministra la seguridad perimetral para la sede de Manizales:

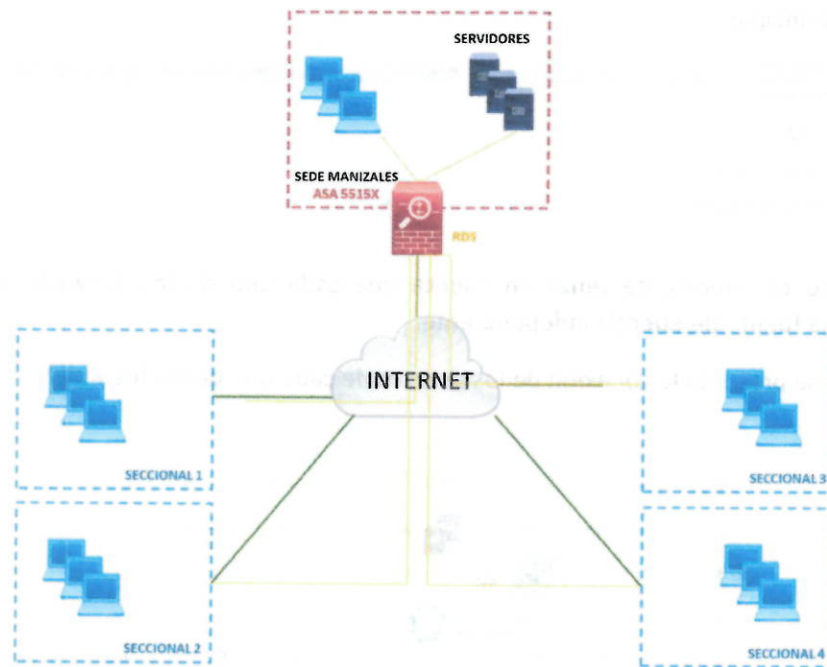
Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos	% completado
FIREWALL ESQUEMA HA	19,43 días	lun 11/02/19	vie 8/03/19		100%
Levantamiento de información y preconfiguración de los switch core para la implementación de los switch core	2 días	lun 18/02/19	mar 19/02/19	Juanita villegas;Angel inglese	100%
Acondicionar switch core para la nueva conexión	2 horas	lun 25/02/19	lun 25/02/19	Juanita villegas	100%
Realizar reimagen de FTD primario y configurar la gestión	3 horas	jue 28/02/19	jue 28/02/19	Juanita villegas;Angel inglese	100%
Realizar reimagen de FTD secundario y configurar la gestión	3 horas	jue 28/02/19	jue 28/02/19	Juanita villegas;Angel inglese	100%
Configurar la gestión de los dos FTD y conectarlos a la red de Empocaldas	1 hora	jue 28/02/19	jue 28/02/19	Juanita villegas;Angel inglese	100%
Realizar configuración de HA entre los dos FTD y conectar los cables	1 hora	jue 28/02/19	jue 28/02/19	Juanita villegas;Angel inglese	100%
Instalación nueva consola FMC	2 horas	vie 1/03/19	vie 1/03/19	Angel inglese	100%
Traducir configuración actual ASA a FTD	12 horas	vie 1/03/19	lun 4/03/19	Angel inglese	100%
configurar FTD secundario en la última imagen con todos sus servicios y migraciones en HA - Transición	6 horas	vie 1/03/19	lun 4/03/19	Angel inglese	100%

Se contaba con el equipo físico instalado y con una máquina virtual desplegada sobre vmware la cual permite gestionar y configurar las reglas de capa 7 de URL filtering y la inspección a nivel de Advanced Malware Protection e IPS.

A nivel del ASDM se administraban las reglas de capa 3 del firewall, por lo que era necesario hacer uso de las dos aplicaciones para realizar una gestión integral del firewall.

La única sede que se encuentra protegida a nivel de firewall es la sede de Manizales. Empocaldas no cuenta con una MPLS, por lo tanto, cada una de las seccionales y plantas navegan directamente a internet sin ningún tipo de protección, lo que implica un gran riesgo de seguridad para la compañía. El RDS (servidor que sirve para que cada una de las seccionales reporte el tema de facturación) esta expuesto sobre internet, con protección del firewall, sin embargo, si hay un robo de identidad se podría tener acceso a los recursos internos de la compañía sin ningún tipo de restricción.

La topología general de las seccionales se muestra en la gráfica a continuación:



Se presentan las siguientes desventajas:

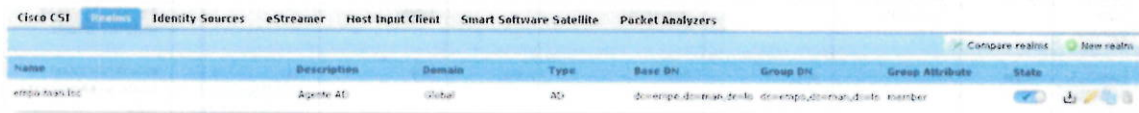
1. No se tiene control de navegación de los usuarios de las seccionales ni plantas, pueden ver cualquier tipo de contenido (Facebook, youtube, streaming de video). Lo cual implica que se realice consumos del ancho de banda de internet y se presente lentitud en los servicios corporativos.
2. No se tiene ningún tipo de seguridad sobre estas máquinas remotas ya que no están registradas en el dominio, no se tiene control sobre la actualización del antivirus, no se tiene visibilidad de lo que sucede sobre estos equipos.
3. El RDS esta publicado a internet, si se presenta un robo de identidad se puede caer en un gran riesgo de seguridad para toda la compañía.

RESUMEN SEGMENTOS DE RED EMPOCALDAS

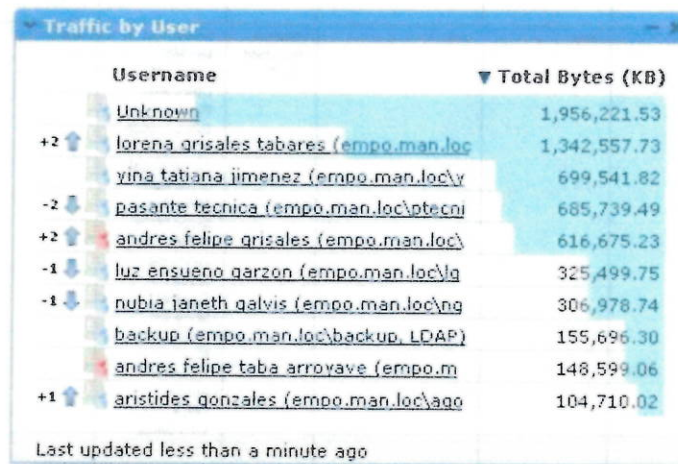
Área	Segmento de Red
Inside	192.168.1.0/24
WLC	192.168.10.0/24
GW_MGMT	192.168.70.0/24
DMZ	192.168.111.0/24

4.2.1. Integración con Directorio Activo

Como parte de las actividades de mejora se realizó la integración de la plataforma de seguridad perimetral con el directorio activo de Empocaldas, lo que permite que se pueda tener visibilidad de los consumos y accesos de los usuarios registrados en el dominio y adicionalmente permite configurar reglas por usuario y no por IP, lo que garantiza facilidad en la administración y asertividad en la configuración de las reglas que se requieran.



Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
empocaldas.loc	Agente AD	Global	AD	dc=empocaldas,dc=loc	dc=empocaldas,dc=loc,dc=users	member	On



Username	Total Bytes (KB)
Unknown	1,956,221.53
+2 lorena_grisales_tabares (empocaldas.man.loc)	1,342,557.73
yina_tatiana_jimenez (empocaldas.man.loc\yina_tatiana_jimenez)	699,541.82
-2 pasante_tecnica (empocaldas.man.loc\otecnica)	685,739.49
+2 andres_felipe_grisales (empocaldas.man.loc\andres_felipe_grisales)	616,675.23
-1 luz_ensueno_garzon (empocaldas.man.loc\luz_ensueno_garzon)	325,499.75
-1 nubia_janeth_galvis (empocaldas.man.loc\nubia_janeth_galvis)	306,978.74
backup (empocaldas.man.loc\backup, LDAP)	155,696.30
andres_felipe_tabararrovave (empocaldas.man.loc\andres_felipe_tabararrovave)	148,599.06
+1 aristides_gonzales (empocaldas.man.loc\aristides_gonzales)	104,710.02

Last updated less than a minute ago

4.2.2. Reglas de Firewall

A continuación se presenta una tabla donde se encuentran las políticas de firewall que estaban configuradas antes de la migración, en la columna de observaciones se encuentra el detalle del ajuste de la regla en los nuevos firewalls instalados.

Name	Action	Source Networks	Original Client Networks	Destination Networks	Users	Application Filters	URLs	OBSERVACIONES
Permit_Secop	Allow	any	any	200.24.63.243	any	any	https://colombiacompra.gov.co/secop-ii https://comunitary.secop.gov.co/formacion.secop.gov.co https://secop.gov.co	Se elimina porque la categoría de secop cambio, ya está categorizado como gobierno.

HABILITAR URL	Allow	any	any	any	any	any	<p>Financial Services (Any Reputation) Government (Any Reputation) Shopping (Any Reputation) www.dian.gov.co www.flickr.com http://ulissesoftware.net/ eps.coomeva.com.co portaleps.coomeva.com.co/portalEPS/portal.php www.community.secop.gov.co http://bfco.falabelladigital.com/payu/Index.html#/login (FallaPay) belalcazar-caldas.gov.co (UriBelalcazar) oferta.senasofiaplus.edu.co/sofia-oferta/ (senasofia) www.sara.unal.edu.co (UNacional) sanjose-caldas.gov.co (UriSanJose) www.procuraduria.gov.co (procuraduria) http://www.corteconstitucional.gov.co/ (Corte) manzanares-caldas.gov.co (UriManzanares) ladorada-caldas.gov.co (UriLaDorada) risaralda-caldas.gov.co (UriRisaralda) www.marulanda-caldas.gov.co (UriMarulanda) anserma-caldas.gov.co (UriAnserma) (Pag_Coomeva) www.palestina-caldas.gov.co (UriPalestina) http://https://bfco.falabelladigital.com/payu/Index.html#/login (FALABELLA_BANCO) filadelfia-caldas.gov.co (UriFiladelfia) victoria-caldas.gov.co (UriVictoria) wetransfer.com (wetransfer) cdimage.debian.org (cdimagen-Debian) www.marquetalia-caldas.gov.co (UriMarquetalia) chinchina-caldas.gov.co (UriChinchina) www.neira-caldas.gov.co (UriNeira) Mozilla UriMarmato UriSamana</p>	Paginas que están categorizadas como gobierno, está permitida por defecto
---------------	-------	-----	-----	-----	-----	-----	--	---

Permit- Redes_so ciales	Allow	192.168.1.141 (EDNA) 192.168.1.168 (JAIRO_GARCIA) 192.168.1.64 (PINTO) 192.168.1.48 (ANDRES_TABA) 192.169.1.159 (jtohon) 192.168.1.68 (MARIA) 192.168.1.178 (MAURICIO_LO ZANO) 192.168.1.65 (MARTHA) 192.168.1.67 (JOHN_JAIRO)	any	any	any	Facebook Facebook Applications Other Facebook Apps Facebook Comment Facebook Like Facebook Message Facebook Notes Facebook Photos Facebook Status Update Facebook event Facebook search Facebook video Instagram Instagram Images Instagram Video YouTube YouTubeMp3 Youtube Upload	any	Esta regla se aplica solamente para los SSID de visitantes y Empo-sistemas. Si
-------------------------------	-------	--	-----	-----	-----	---	-----	--

FTP-AMP	Allow	any	any	any	any	FTP FTP Data	any	Ya se está inspeccionando por defecto
Permit_C olpension es	Allow	any	any	any	User:emp o.man.loc /cmcanda mil	any	www.colpensiones.gov.co	Paginas que están categorizadas como gobierno, está permitida por defecto
Acces_So fiaplus	Allow	any	any	any	any	any	senasofiaplus.edu.co http://portal.senasofiaplus.edu.co/ http://auth.senasofiaplus.edu.co/	Paginas que están categorizadas como gobierno, está permitida por defecto
Permit- SIVICAP	Allow	any	any	any	User:emp o.man.loc /ngalvis.e mpo.man .loc/ptec nica	any	aplicacionespruebas.ins.gov.co (SIVICAP)	Paginas que están categorizadas como gobierno, está permitida por defecto
Permitido s- Autorizad os	Allow	any	any	any	any	Google Play Eset Google APIs Google Accounts Authentication Google App Engine Google Checkout Google Desktop Google Drive Google Inbox Google Sign in	any	Se crea regla que permite las aplicaciones de Google
ACCESO_ SIS	Allow	192.168.1.0/24 192.168.110.0/ 24 192.168.111.0/ 24 (RedesInternas)	any	any	User:emp o.man.loc /jigiraldo, empo.ma n.loc/mg uzman,e mpo.man .loc/rapin tor,empo. man.loc/j tobon	YouTube Youtube Upload	any	Esta regla no estaba funcionando

HABILITA R APP	Allow	any	any	any	any	Eset Firefox Java Java RMI Java Update Mozilla Skype Photo (Deprecated) Skype Video (Deprecated) Skype Video Message (Deprecated) Skype Voice (Deprecated) WeTransfer WebEx WebEx Connect WebEx Media WebEx Sharing Windows Live Windows Live Hotmail Windows Live SkyDrive	any	Esta habilitada por defecto
Políticas_ Servidores	Allow	any	any	192.168.111.23 (Rem-Desktop) 192.168.1.8 (Dominio) 192.168.1.18 (GestionCintasLto) 192.168.1.25 (SolIn) 192.168.1.15 (Fortuner)	any	any	any	Regla que es aplicada por defecto
URLS no categorizadas	Interactivo Block with Reset	any	any	any	any	any	ipornogratias.xxx pornogratiasdiario.com serviporno.com/ donpornogratias.com	Están bloqueadas por defecto

License

Base:	Yes
Export-Controlled Features:	Yes
Malware:	Yes
Threat:	Yes
URL Filtering:	Yes

Estas licencias fueron adquiridas por un periodo de 12 meses.

4.2.4. Direcccionamiento IP

Para la administración y gestión de los equipos se utilizó el siguiente direccionamiento IP

A continuación se encuentra la lista de las direcciones IP configurada a los equipos de red LAN y firewall:

RESUMEN DIRECCIÓN IP - FTD

Interface	Logical Name	Type	Security Zones	NA...	IP Address
Diagnostic1/1	management	Physical			192.168.254.1/255.255.255.0(Static)
GigabitEthernet1/1	Outside-LU/E	Physical	Outside-LU/E 1.Interface_Group		181.129.131.2/255.255.255.248(Static)
GigabitEthernet1/2	DMZ	Physical	DMZ 1.Interface_Group		192.168.111.1/255.255.255.0(Static)
GigabitEthernet1/3	Inside	Physical	Inside 1.Interface_Group		192.168.1.1/255.255.255.0(Static)
GigabitEthernet1/3.3	Inside-VLC	SubInterface	Inside-VLC 1.Interface_Group		192.168.10.294/255.255.255.0(Static)
GigabitEthernet1/4	GW-MGMT	Physical	GW-MGMT 1.Interface_Group		192.168.70.1/255.255.255.0(Static)
GigabitEthernet1/5	DMZ-110	Physical	DMZ-110 1.Interface_Group		192.168.110.1/255.255.255.0(Static)
GigabitEthernet1/6	Outside-2CapCom	Physical	Outside-2CapCom 1.Interface_Group		143.137.94.66/255.255.255.248(Static)
GigabitEthernet1/7		Physical			
GigabitEthernet1/8		Physical			

IP GESTIÓN

SWITCH NAME	IP	SERIAL	MODELO
FTD PRINCIPAL	192.168.70.101	JAD225208YB	Cisco ASA5508-X Threat Defense
FTD PRINCIPAL	192.168.70.102	JAD22520957	Cisco ASA5508-X Threat Defense
FIREPOWER	192.168.70.100	Cisco Firepower Management Center for VMWare	Versión: 6.3.0.1

EMPRESA DE OBRAS SANITARIAS DE CALDAS S.A E.S.P
EMPOCALDAS S.A E.S.P

NIT 890.803.239-9

REGISTRO PRESUPUESTAL

NUMERO 000278

FECHA DE EXPEDICION 2019/02/08
CERTIFICADO DISPON. NRO - 000266
COMPROMISO QUE AMPARA CONTRATO PRESTACION DE SERVICIOS N° 0089/19 FORTALECIMIENTO DEL SISTEM
A DE PROTECCION CONTRA ATAQUES INFORMATICOS A LA EMPRESA
BENEFICIARIO DATA & SERVICE
C.C NRO 810001025

Con el presente acto administrativo se afecta de manera definitiva, la(s) apropiacion(es) y no serán utilizados con otro fin. (Requisito de perfeccionamiento y anterior a la ejecucion).

RUBRO APROPIACION	DESCRIPCION	VALOR
21020225	SISTEMATIZACIÓN	127,115,071
TOTAL REGISTRO PRESUPUESTAL		127,115,071

PLAZO DE EJECUCION 30 DIAS


JOSE OSCAR BEDOYA AGUIRRE
Jefe Sección Presupuesto