	F-GC-29 Versión 2 Septiembre 2019	EMPOCALDAS S.A E.S.P GESTIÓN DE CONTRATACIÓN
		LISTA CHEQUEO PAGO DE ACTAS - CONTRATOS PRESTACIÓN DE SERVICIOS Y CONSULTORIA

# CONTRATO Y AÑO	0041/2019	Acta N°	8	1. VALOR INICIAL (incluido IVA)	60.000.000
				2. VALOR ADICION (+)	
CONTRATISTA	DATA & SERVICE LTDA			3. VALOR TOTAL (1+2)	60.000.000
NIT O CC:	810001025-7			4. VALOR ACTAS ANTERIORES (-)	35.000.000
CDP (#, rubro y fecha)	0073 DE 01 DE ENERO DE 2019			5. VALOR PRESENTE ACTA (-)	5.000.000
RP (#, rubro y fecha)	0133 DE 15 DE ENERO DE 2019			6. VALOR NO EJECUTADO (3 - 4 - 5)	20.000.000

OBJETO DEL CONTRATO: PRESTACION DE SERVICIOS PROFESIONALES PARA ADMINISTRAR, OPTMIZAR, ASEGURAR Y DAR SOPORTE A LOS RECURSOS DEL CENTRO DE COMPUTO, RED DE DATOS, SISTEMAS DE SEGURODAD INFORMATICA DE BACKUP Y RESTAURACION.

TIPO DE RECURSOS	PROPIOS	CENTRO DE COSTOS y PROCEDIMIENTO	

DOCUMENTO VERIFICADOS	√	# FOLIOS
1- Acta original	X	
2- 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).	NA	
3- Tarjeta profesional y certificado de la Junta Central de contadores con fecha de expedición no mayor a tres meses (aplica cuando el certificado de parafiscales lo firma el Revisor Fiscal o el Contador).	NA	
4- Factura (Régimen Común) o Factura equivalente (régimen simplificado).	X	
5- Pagos SENA y ICBF.	NA	
6- Evaluación del Supervisor Formato F-GC-18 (Solo aplica para el acta final)	NA	
7- Planillas de pago con firma de los trabajadores (cuando se cuente con personal a cargo).	NA	
8- 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.

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

Juan Camilo A. — NOMBRE DE QUIEN RECIBE

23/11/2019 — FIRMA

DOCUMENTOS ANEXOS CON DESTINO A TESORERÍA	√
Copia del Acta	X
Factura (Régimen Común) o Factura equivalente (régimen simplificado).	
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).	
Distribución por centro de costos. Formato F-GF-32	

Fecha de presentación 15/11/2019

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

DATOS PARA LA TRANSFERENCIA DE PAGOS		
5902062602	CORRIENTE	BANCOLOMBIA
CUENTA	TIPO DE CUENTA	BANCO

ACTA DE RECIBO # 8

CONTRATO	No. 0041/2019
OBJETO	PRESTACION DE SERVICIOS PROFESIONALES PARA ADMINISTRAR, OPTIMIZAR, ASEGURAR Y DAS SOPORTE A LOS RECURSOS DEL CENTRO DE COMPUTO, RED DE DATOS, SISTEMAS DE SEGURIDAD INFORMATICA, DE BACKUP Y RESTAURACION
CONTRATISTA	DATA & SERVICE LTDA
VALOR CONTRATO	$60.000.000
RECURSOS	PROPIOS

En la ciudad de Manizales a los quince (15) días del mes de noviembre 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. 8 al Contrato No. 0041 de 2019.

VALOR CONTRATO	$60.000.000
ACTA # 1	$5.000.000
ACTA # 2	$5.000.000
ACTA # 3	$5.000.000
ACTA # 4	$5.000.000
ACTA # 5	$5.000.000
ACTA # 6	$5.000.000
ACTA # 7	$5.000.000
ACTA # 8	$5.000.000
VALOR EJECUTADO	$40.000.000
VALOR POR EJECUTAR	$20.000.000

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

FERNANDO BETANCOURT E.
Representante Legal
DATA & SERVICE LTDA.

Preparó: Juan David Tirado

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 trece (13) días del mes de noviembre (11) del año dos mil diecinueve (2019).

FERNANDO BETANCOURT ESCOBAR
C.C. 10.278.051

PBX 8812277
www.datayservice.com
Manizales

Data&Service

"Un Servidor en Quien Confiar"

data & service
NIT. 810001025-7

FACTURA DE VENTA No.: 12360

CALLE 54 No. 26-60
MANIZALES
NIT: 810.001.025-7
TEL: 8812277

FECHA: 2019/11/13

IVA REGIMEN COMÚN

Presente su factura
Para hacer efectiva
su garantía.
informacion@datayservice.com

Información del Cliente:

NOMBRE : EMPOCALDAS S.A. E.S.P
DIRECCION: CRA. 23 NRO. 75-82
CIUDAD : MANIZALES
VENDEDOR : 04

NIT/CC : 890803239
TEL/FAX: 8867080

VENCE : 2019 12 13

UNIDADES	DESCRIPCION	VALOR UNITARIO	VALOR NETO
1	Servicios para Administrar	5,000,000.00	5,000,000.00
1	Optimizar, Asegurar y dar	0.00	0.00
1	Soporte a los Recursos del	0.00	0.00
1	Centro de Cómputo, Red Datos	0.00	0.00
1	Sistema Seguridad Informática	0.00	0.00
1	Backup y Restauración	0.00	0.00

EMPOCALDAS S.A. E.S.P
Radicado número:
2019-EI-00004402
14/11/2019 11:40:37 AM **Folios** 2

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

Observaciones

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

CONTRATO No. 0041 DE 2019

FIRMA Y SELLO ALMACÉN

Recibido

Firma Documento o Sello

SUBTOTAL	$	5,000,000
RETEICA	$	0.00
RETENCION	$	0
RETEIVA	$	0
IVA	$	0.00
TOTAL	$	5,000,000

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.

INFORME DE SUPERVISION

CONTRATO	Nº 0041/2019
CONTRATISTA	DATA & SERVICE LTDA
OBJETO	PRESTACION DE SERVICIOS PROFESIONALES PARA ADMINISTRAR, OPTIMIZAR, ASEGURAR Y DAR SOPORTE A LOS RECURSOS DEL CENTRO DE COMPUTO, RED DE DATOS, SISTEMAS DE SEGURIDAD INFORMATICA, DE BACKUP Y RESTAURACION LICENCIA Y SOPORTE EQUIPO DE SEGURIDAD PERIMETRAL, SISTEMA DE VIRTUALIZACION.
VALOR	$60.000.000
RECURSOS	EMPOCALDAS S.A E.S. P

En cumplimiento del contrato 0041/2019, cuyo objeto es PRESTACION DE SERVICIOS PROFESIONALES PARA ADMINISTRAR, OPTIMIZAR, ASEGURAR Y DAR SOPORTE A LOS RECURSOS DEL CENTRO DE COMPUTO, RED DE DATOS, SISTEMAS DE SEGURIDAD INFORMATICA, DE BACKUP Y RESTAURACIONACION LICENCIA Y SOPORTE EQUIPO DE SEGURIDAD PERIMETRAL, SISTEMA DE VIRTUALIZACION, se evidenció que dicho contrato se desarrolló satisfactoriamente a los términos y especificaciones del contrato según el objeto contractual mencionado y cumplió con los pagos por concepto de seguridad social y parafiscales, cumplen también con las afiliaciones a salud, pensiones, cesantías y riesgos profesionales.

VALOR CONTRATO	$60.000.000
ACTA # 1	$5.000.000
ACTA # 2	$5.000.000
ACTA # 3	$5.000.000
ACTA # 4	$5.000.000
ACTA # 5	$5.000.000
ACTA # 6	$5.000.000
ACTA # 7	$5.000.000
ACTA # 8	$5.000.000
VALOR EJECUTADO	$40.000.000
VALOR POR EJECUTAR	$20.000.000

Manizales, 15 de noviembre de 2019

JOHN JAIRO GIRALDO VILLA
Jefe Sección Sistemas
Supervisor

Preparó: Juan David Tirado Buitrago

Data & Service

empocaldas

Manizales, noviembre 11 del 2019

Señores

EMPOCALDAS
Atn. Ing. John Jairo Giraldo Jaramillo.
Sistemas

Asunto: **INFORME ESTADO INFRAESTRUCTURA PERIODO OCTUBRE**

Por medio de este informe queremos poner al servicio de EMPOCALDAS, todo el conocimiento y la experiencia transmitida durante el contrato de mantenimiento efectuado con nuestra compañía DATA & SERVICE. Dentro de las labores contractuales adquiridas por nuestra empresa se describen de la siguiente forma:

Soporte a plataformas en producción en ambientes de virtualización Vmware, Hyper-v y Baremetal Windows server 2012, listados a continuación:

Sistema de Backup
IBM Blade Center S con las siguientes cuchillas
i. Vmware 6 - 192.168.70.16
ii. Vmware 6 – 192.168.70.17
iii. Vmware 5 – 192.168.70.14
iv. Windows Server 2012 – 192.168.1.20
IBM Systemx Server con sistema operativo Windows Server 2012 – 192.168.1.18
Cisco UCS Server con Vmware 6 - 192.168.70.19

Soporte plataforma de Seguridad perimetral cisco con los siguientes componentes:

Firewall Físico Cisco *ASA5508-X* con módulo firepower - 192.168.70.101 – 192.168.70.102
Firewall de Aplicaciones SourceFire Manager – 192.168.70.100

Agradecemos haber sido tenidos en cuenta y estaremos atentos para resolver cualquier inquietud al respecto.

Juan Camilo Salinas Sepúlveda
Equipo Infraestructura

cisco partner · arcserve · FORTINET · KASPERSKY · Windows Server · VoIbox

Data & Service

empocaldas

Servidor Cisco C240-M5

El servidor de rack Cisco UCS C240 M5 es un servidor de rack de 2 sockets y 2 unidades de rack (2RU) que ofrece un rendimiento y capacidad de expansión líderes en la industria. Admite una amplia gama de cargas de trabajo de infraestructura intensivas de almacenamiento y E / S, desde big data y análisis hasta colaboración. Los servidores en rack Cisco UCS serie C pueden implementarse como servidores independientes o como parte de un entorno administrado Cisco Unified Computing System ™ (Cisco UCS) para aprovechar las innovaciones informáticas unificadas basadas en estándares de Cisco que ayudan a reducir el costo total de propiedad (TCO) de los clientes) y aumentar su agilidad empresarial.

El regulador de la administración integrada del servidor Cisco denominado "CIMC" se puede acceder a través de la URL https://192.168.1.6/login.html en donde encontraran las diferentes propiedades y configuración del servidor.

Propiedades del servidor

Nombre del prod...	UCS C240 M5SX
Número de serie:	WZP2332088N
PID:	UCSC-C240-M5SX
UUID:	E1625C5E-938A-42B4-81E7-66834E7049B9
Versión BIOS:	C240M5.4.0.4c.0.0411190411
Descripción:	
Etiqueta de recur...	Unknown

Información del Regulador de la administración integrada de Cisco (Cisco IMC)

Nombre de host:	C240-WZP2332088N
Dirección IP:	192.168.1.6
Dirección MAC:	2C:F8:9B:4D:3E:70
Versión de firmware:	4.0(4b)
Hora actual (UTC):	Wed Oct 23 19:09:04 2019
Hora local:	Wed Oct 23 14:09:04 2019 COT -0500
Zona horaria:	America/Bogota

Seleccionar zona horaria

Unidades virtuales

Seleccionado 0 / Total 2

	Número de unidad virtual	Nombre	Estado	Estado general	Tamaño	Nivel de R...	Unidad de...
☐	0	RAID_6	Optimal	Good	6862608 MB	RAID 6	false
☐	1	RAID_1	Optimal	Good	456809 MB	RAID 1	true

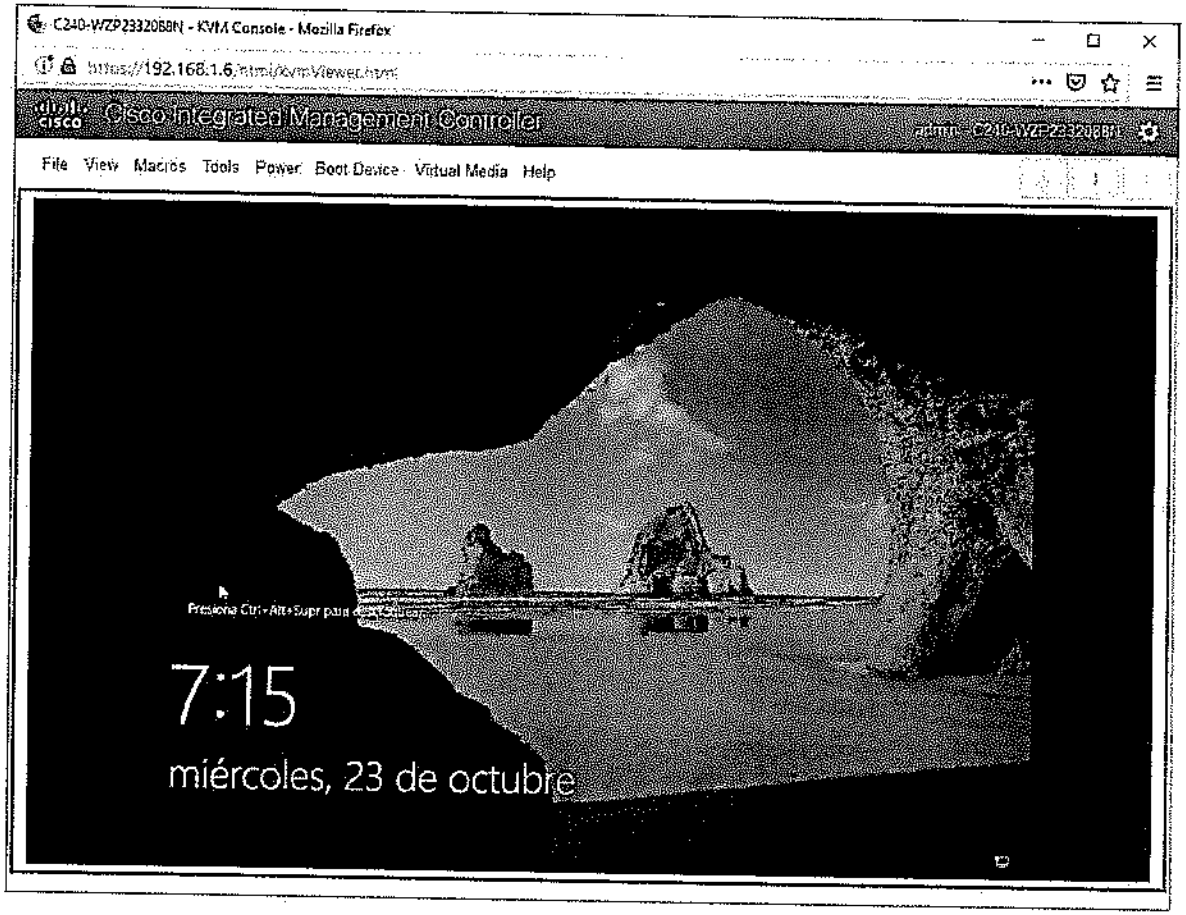
arcserve FORTINET KASPERSKY Windows Server Hyper-V VirtualBox

Data & Service

empocaldas

KVM Launch Manager – Cisco UCS

La consola KVM es una interfaz accesible desde la GUI de Cisco UCS Manager o KVM Launch Manager que emula una conexión KVM directa. A diferencia del dongle KVM, que requiere estar físicamente conectado al servidor, la consola KVM le permite conectarse al servidor desde una ubicación remota a través de la red.



Data & Service

empocaldas

Sistema Operativo

Windows Server 2019 Standard

Sistema

Procesador:	Intel(R) Xeon(R) Gold 5118 CPU @ 2.30GHz 2.29 GHz (2 procesadores)
Memoria instalada (RAM):	256 GB (256 GB utilizable)
Tipo de sistema:	Sistema operativo de 64 bits, procesador x64
Lápiz y entrada táctil:	La entrada táctil o manuscrita no está disponible para esta pantalla

Configuración de nombre, dominio y grupo de trabajo del equipo

Nombre de equipo:	EMPOBK
Nombre completo de equipo:	EMPOBK.empo.man.loc
Descripción del equipo:	
Dominio:	empo.man.loc

Cambiar configuración

Activación de Windows

Windows está activado Lea los Términos de licencia del software de Microsoft

Id. del producto: 00431-10000-00000-AA862

Cambiar la clave de producto

arcserve FORTINET KASPERSKY Windows Server VolBox

Data & Service

empocaldas

Arcserve Unified Data Protection

Arcserve Unified Data Protection (UDP) combina tecnologías probadas de recuperación de desastres, backup y verdadera deduplicacion global en una solución unificada que ofrece todas las funcionalidades de protección de datos que usted y su empresa necesitan.

Potenciada por una tecnología heterogénea basada en imágenes que brinda protección desde y hacia cualquier objetivo, esta solución unifica funcionalidades listas para las grandes empresas sin la complejidad de las soluciones tradicionales.

Arcserve Unified Data Protection
Version: 7.0.4455
Update 1 Build 392

Licenciamiento

Your Arcserve product has been activated.

To change your information, edit it below and click Update. If Email Address is changed, a verification email will be sent to the new address within one hour.

* Indicates a required field

* Email Address: sistemas@empocaldas.com.co

Arcserve UDP Licenses

License Name	Total	Remaining	Unlicensed
Arcserve UDP 7.0 Premium Edition - Socket	4	4	0
Arcserve UDP 7.0 Premium Plus Edition - Socket	4	4	0

La herramienta de respaldo Arcserve UDP es el nivel de seguridad de la información más alto que tiene la compañía, determinando planes de retención de la información utilizada para el correcto funcionamiento de la empresa. Se tiene una consola de administración la cual muestra el estado actual de las copias de seguridad en disco.

cisco Partner · arcserve · FORTINET · KASPERSKY · Windows Server Hyper-V · Veeam

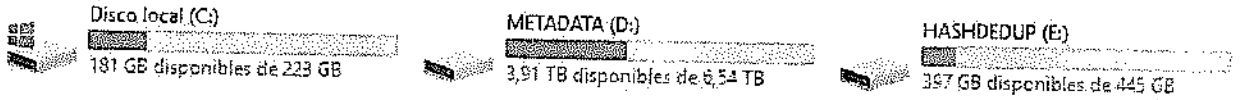
El Datastore configurado en el cual se almacenará la información de la compañía es el siguiente:

Destinations: Recovery Point Server

Actions | Add a Recovery Point Server

Name	Status	Plan Count	Stored Data	Deduplication	Compression	Overall Data Reduction	Space Occupied
empobk.emdo.man.loc							
DS_EMPOBK		1	3.78 TB	46%	31%	63%	1.41 TB

Los datos estarán almacenados en el servidor 192.168.1.10 "EMPOBK" de la siguiente manera:



- **Se tiene un disco local (D:) METADATA** – Donde se tiene configurada la DATA de la compañía.

Este equipo › METADATA (D:) › DS_EMPOBK ›

Nombre	Fecha de modifica...	Tipo
DS_DATA	21/10/2019 7:32 p....	Carpeta de archivos
DS_DESTINATION	22/10/2019 10:08 ...	Carpeta de archivos
DS_INDEX	21/10/2019 7:32 p....	Carpeta de archivos

- **Se tiene un disco local (E:)** – Donde se tiene configurado el Data Store ILC

Este equipo › HASHDEDUP (E:) › DS_EMPOBK ›

Nombre	Fecha de modifica...	Tipo
DS_HASH	21/10/2019 7:32 p....	Carpeta de archivos

Data & Service

empocaldas

Planes de retención

Se configura el plan de backup de los servidores de la siguiente manera:

1. Se realizará un backup diario a las 6:45 PM *(Se almacenarán los últimos 7 días de cada servidor)*
2. Se realizará un backup semanal el cual se realizará el sábado a las 10:00 PM *(Se almacenarán las últimas 5 semanas de cada servidor)*
3. Se realizará un backup mensual el cual se realizará el 2 día de cada mes a las 11:00 PM *(Se almacenarán los últimos 6 meses de cada servidor)*

Type	Description	Su	Mo	Tu	We	Th	Fr	Sa	Time
	Daily Incremental Backup		✔	✔	✔	✔	✔		6:45 PM
	Weekly Incremental Backup							✔	10:00 PM
	Monthly Incremental Backup							1/12	11:00 PM

First backup (Full Backup): 12/10/2019 5 : 00 PM

Recovery Point Retention

Daily Backups	7
Weekly Backups	5
Monthly Backups	6
Custom / Manual Backups	4

NOTA: La plataforma de backup tiene un periodo de estabilización de 1 semana, en la cual se estarán realizando cambios de fechas, horarios y días de retención, con el fin de brindar la mejor cobertura posible en cuestión de tareas de backup y restauración, afectando lo menos posible los servicios de la compañía.

cisco arcserve FORTINET KASPERSKY Windows Server Hyper-V Veeam

Data & Service

empocaldas

Lista de servidores protegidos actualmente

Nodes: All Nodes

Actions | Add Nodes | Filter (Filter applied)

Status	Node Name	VM Name	Plan	Hypervisor	Last Backup Result	Last Backup Time
✓	admi-archi.empo.man.loc	ADMIN-ARCHI	PLAN_BK_EMPO	192.168.70.16	Finished	24/10/2019 8:09:35 PM
✓	copiabdsolin.empo.man.loc	COPIABDSOLIN	PLAN_BK_EMPO	192.168.70.19	Finished	25/10/2019 7:39:23 AM
✓	dominio.empo.man.loc	DAEMPO	PLAN_BK_EMPO	192.168.70.14	Finished	24/10/2019 7:57:13 PM
✓	fmc-01.empo.man.loc	Firepower - FTD	PLAN_BK_EMPO	192.168.70.19	Finished	24/10/2019 7:18:01 PM
✓	fortuner2018.empo.man.loc	ERP-FORTUNER-2018	PLAN_BK_EMPO	192.168.70.16	Finished	24/10/2019 6:47:13 PM
✓	intranet.empo.man.loc	INTRANET_1	PLAN_BK_EMPO	192.168.70.16	Finished	24/10/2019 7:33:00 PM
✓	n32.empo.man.loc	N32	PLAN_BK_EMPO	192.168.70.19	Finished	24/10/2019 7:25:25 PM
✓	nominasql.empo.man.loc	NOMINA SQL	PLAN_BK_EMPO	192.168.70.14	Finished	24/10/2019 6:47:13 PM
✓	rds.empo.man.loc	EMPOCALDAS-RDS	PLAN_BK_EMPO	192.168.70.19	Finished	24/10/2019 7:45:44 PM
✓	solinapp2018.empo.man.loc	SolinAPP2018	PLAN_BK_EMPO	192.168.70.14	Finished	24/10/2019 7:24:51 PM
✓	solindb.empo.man.loc	Solin 2015 Win 2012 SQL2012	PLAN_BK_EMPO	192.168.70.17	Finished	24/10/2019 7:47:53 PM
✓	webdmz.empo.man.loc	DMZ_SIICO	PLAN_BK_EMPO	192.168.70.19	Finished	24/10/2019 6:47:13 PM

NOTAS:

- *Actualmente se tienen 12 servidores Virtuales respaldados por la herramienta Arscerve UDP, con backup del día 24 de octubre de 2019*
- *En el momento se tiene 1 Data Store (DS_EMPOBK) que soportara la operación en el servidor 192.168.1.10 en los discos D y E.*
- *Los servidores administrados en la plataforma están disponibles para tareas de restauración desde este momento.*

cisco Select Partner · arcserve · FORTINET · KASPERSKY · Windows Server Hyper-V · Volbox

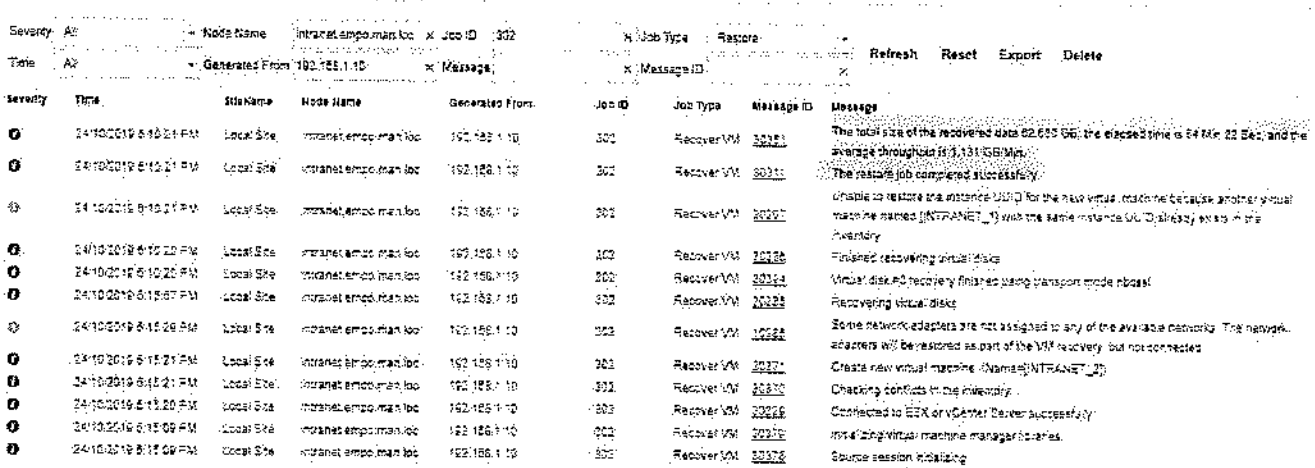
Data & Service

empocaldas

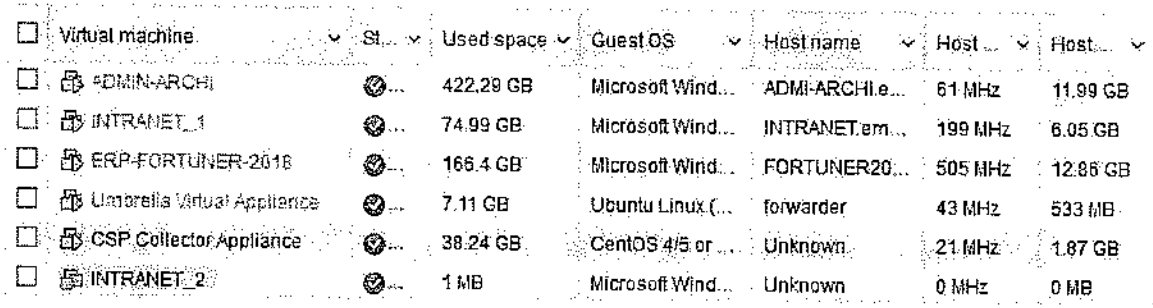
Arcserve Unified Data protection - Restauracion

Se dispone a realizar pruebas de restauración desde disco las cuales arrojan el siguiente resultado:

1. La restauración se realiza correctamente
2. Tiempo de restauración. 54 minutos, 22 Segundos.
3. Velocidad de transferencia de datos: 1.131GB/min
4. Total, de datos restaurados: 62.680GB



Severity	Time	SiteName	Node Name	Generated From	Job ID	Job Type	Message ID	Message
0	24/10/2019 6:19:21 PM	Local Site	intranet.empo.main.loc	192.168.1.10	302	Recover VM	32781	The total size of the recovered data 62.680 GB, the elapsed time is 54 Min. 22 Sec, and the average throughput is 1.131 GB/Min.
0	24/10/2019 6:19:21 PM	Local Site	intranet.empo.main.loc	192.168.1.10	302	Recover VM	32811	The restore job completed successfully.
0	24/10/2019 6:19:21 PM	Local Site	intranet.empo.main.loc	192.168.1.10	302	Recover VM	32807	Unable to restore the instance UUID for the new virtual machine because another virtual machine named [INTRANET_1] with the same instance UUID already exists in the inventory.
0	24/10/2019 6:19:20 PM	Local Site	intranet.empo.main.loc	192.168.1.10	302	Recover VM	32736	Finished recovering virtual disks.
0	24/10/2019 6:19:20 PM	Local Site	intranet.empo.main.loc	192.168.1.10	302	Recover VM	32734	Virtual disk #0 recovery finished using transport mode nbssl.
0	24/10/2019 6:15:57 PM	Local Site	intranet.empo.main.loc	192.168.1.10	302	Recover VM	32729	Recovering virtual disks.
0	24/10/2019 6:15:29 PM	Local Site	intranet.empo.main.loc	192.168.1.10	302	Recover VM	32668	Some network adapters are not assigned to any of the available networks. The network adapters will be restored as part of the VM recovery, but not connected.
0	24/10/2019 6:15:21 PM	Local Site	intranet.empo.main.loc	192.168.1.10	302	Recover VM	32727	Create new virtual machine. (Name:[INTRANET_2])
0	24/10/2019 6:15:21 PM	Local Site	intranet.empo.main.loc	192.168.1.10	302	Recover VM	32670	Checking conflicts in the inventory.
0	24/10/2019 6:15:20 PM	Local Site	intranet.empo.main.loc	192.168.1.10	302	Recover VM	32726	Connected to ESX or vCenter Server successfully.
0	24/10/2019 6:15:09 PM	Local Site	intranet.empo.main.loc	192.168.1.10	302	Recover VM	32676	Initializing virtual machine manager libraries.
0	24/10/2019 6:15:09 PM	Local Site	intranet.empo.main.loc	192.168.1.10	302	Recover VM	32675	Source session initializing.



Virtual machine	St...	Used space	Guest OS	Host name	Host ...	Host...
ADMIN-ARCHI	...	422.29 GB	Microsoft Wind...	ADMI-ARCHI.e...	61 MHz	11.99 GB
INTRANET_1	...	74.99 GB	Microsoft Wind...	INTRANET.em...	199 MHz	6.05 GB
ERP-FORTUNER-2018	...	166.4 GB	Microsoft Wind...	FORTUNER20...	505 MHz	12.86 GB
Umbrella Virtual Appliance	...	7.11 GB	Ubuntu Linux (...	forwarder	43 MHz	533 MB
CSP Collector Appliance	...	38.24 GB	CentOS 4/5 or ...	Unknown	21 MHz	1.87 GB
INTRANET_2	...	1 MB	Microsoft Wind...	Unknown	0 MHz	0 MB

arcserve FORTINET KASPERSKY Windows Server Hyper-V Veeam

Data & Service

empocaldas

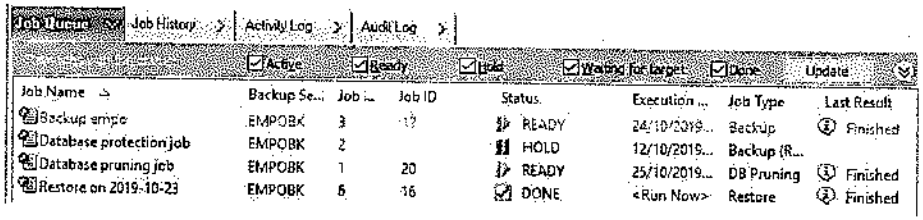
Arcserve Backup

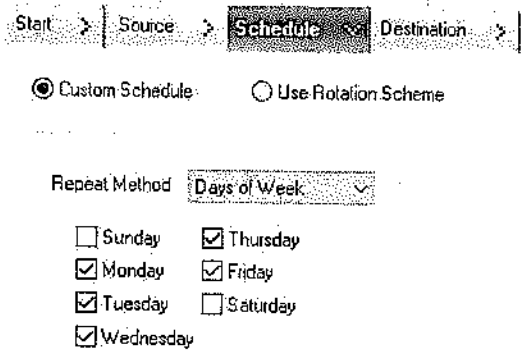
Arcserve manipula las copias de seguridad en cinta de forma diferente con una tecnología única que mejora la economía de protección de datos haciendo posible que haya periodos de retención más prolongados, reduciendo el almacenamiento e integrando una deduplicacion potente en el entorno de copias de seguridad que ya tengas.

Guarda datos críticos en prácticamente cualquier dispositivo de cinta, desde una unidad de cinta individual hasta bibliotecas de cintas enormes. Gestiona más datos en más ubicaciones Pasa menos tiempo gestionando copias de seguridad, independientemente de lo sencilla o compleja que pueda ser tu infraestructura.

Tareas de Backup

1. Se programa una tarea de backup a cinta la cual se aplica los días, lunes, martes, miércoles, jueves y viernes.



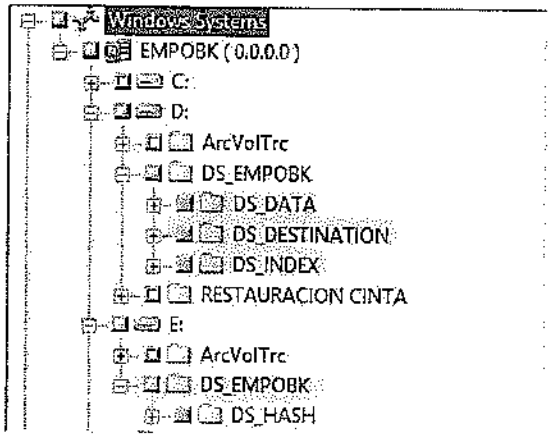


arcserve FORTINET KASPERSKY Windows Server Hyper-V Volbox

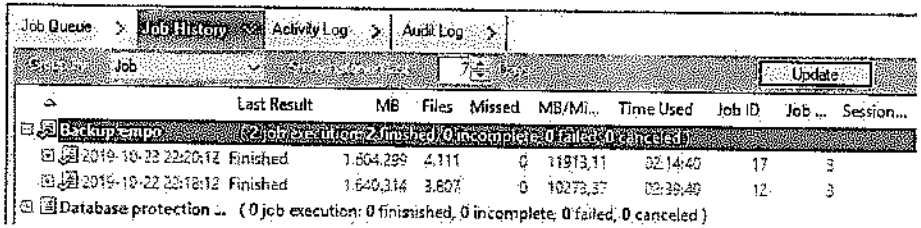
Data & Service

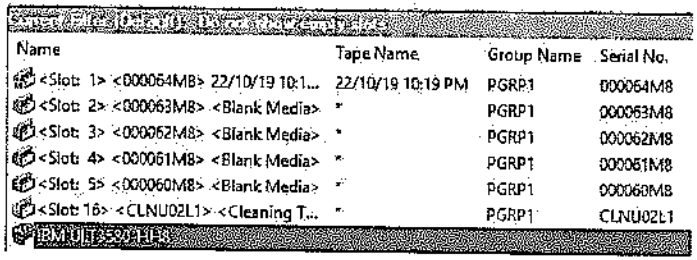
empocaldas

2. Se están protegiendo en cinta las siguientes unidades:



3. Se dispone a activar las tareas de backup a cinta, las cuales funcionan correctamente.





arcserve FORTINET KASPERSKY Windows Server Veeam

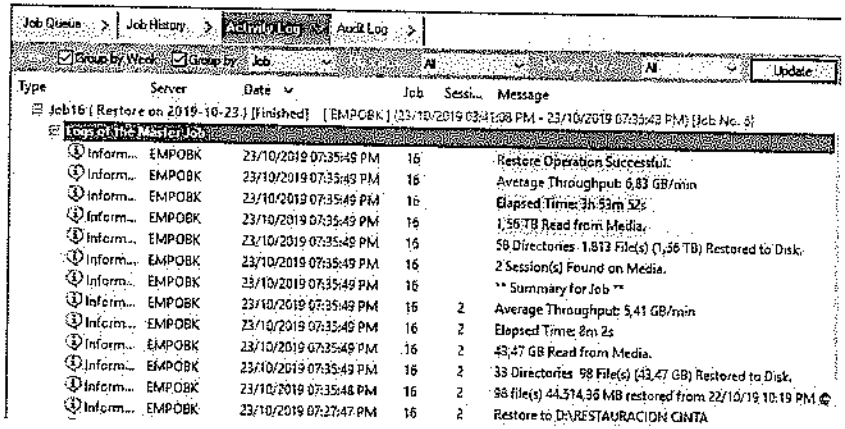
Data & Service

empocaldas

Arcserve Backup - Restauracion

Se dispone a realizar pruebas de restauración desde cinta las cuales arrojan el siguiente resultado:

5. La restauración se realiza correctamente
6. Tiempo de restauración. 3Horas, 53 Minutos, 52 Segundos.
7. Velocidad de transferencia de datos: 6.83GB/min
8. Total, de datos restaurados: 2.56TB

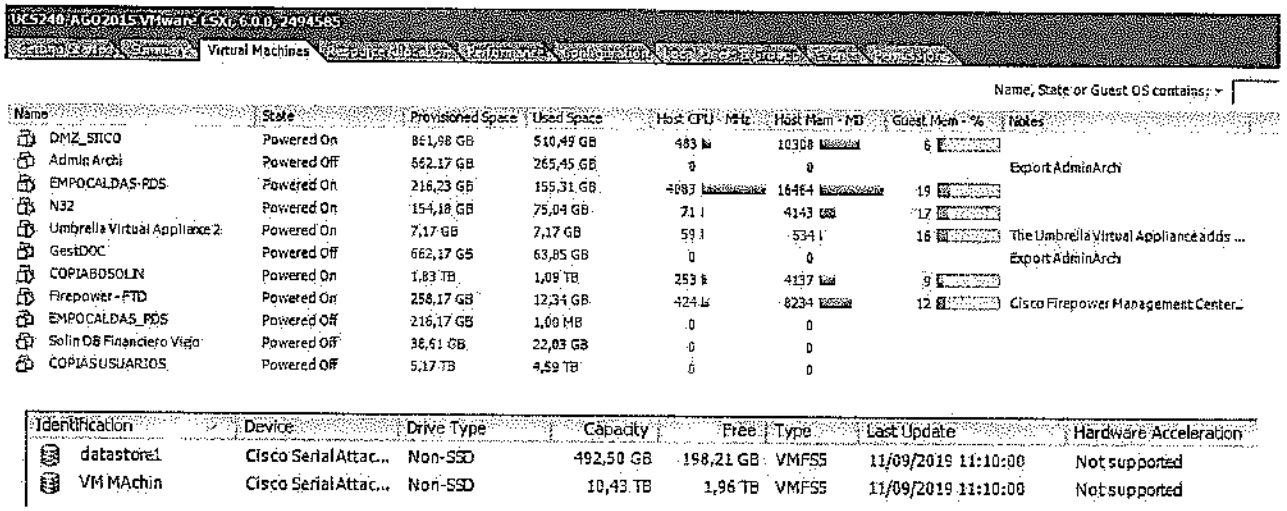


arcserve FORTINET KASPERSKY Windows Server Hyper-V Veeam

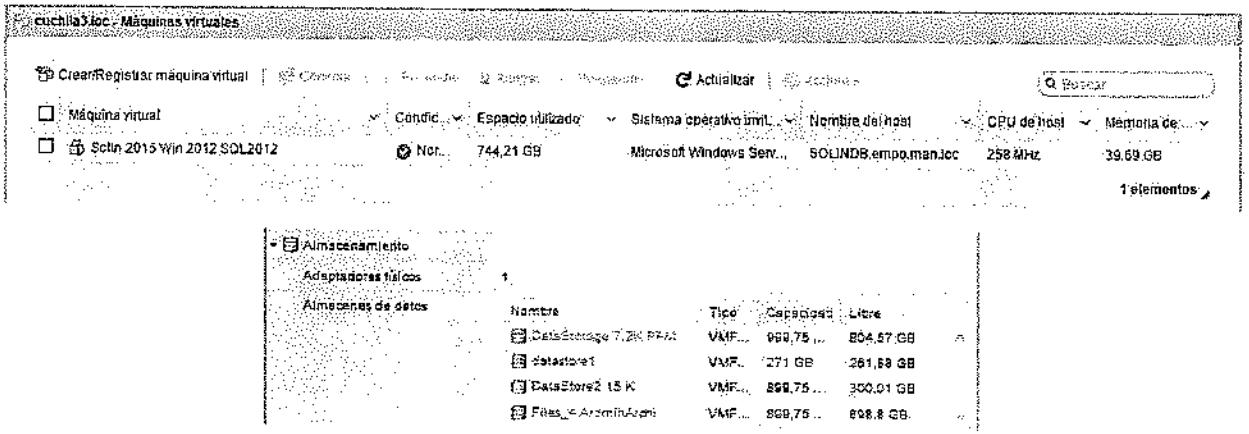
Data & Service

empocaldas

Estado de los ambientes - servidores



Cuchilla 3



cisco Partner

arcserve

FORTINET

KASPERSKY

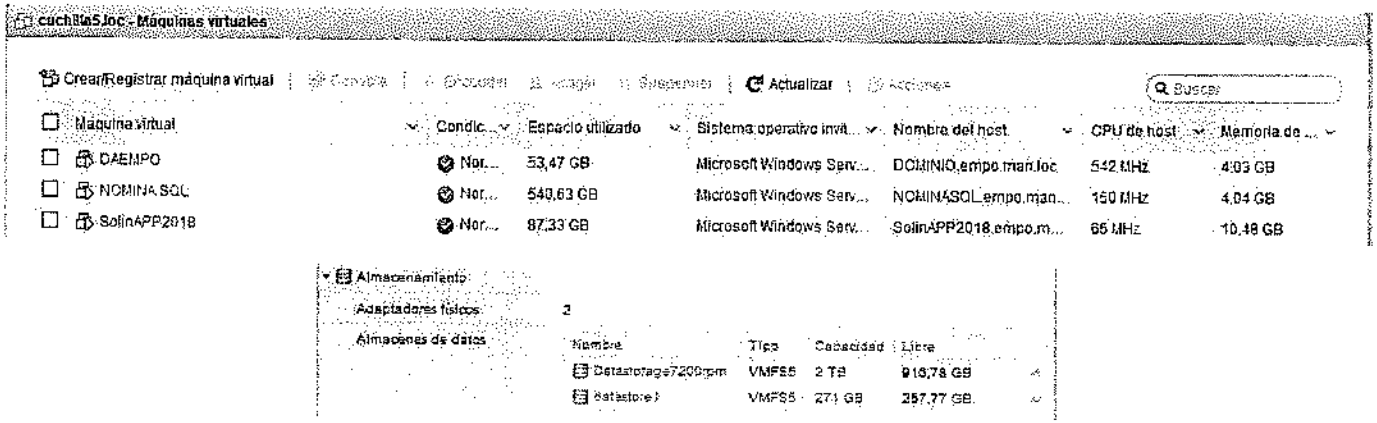
Windows Server Hyper-V

Volbox

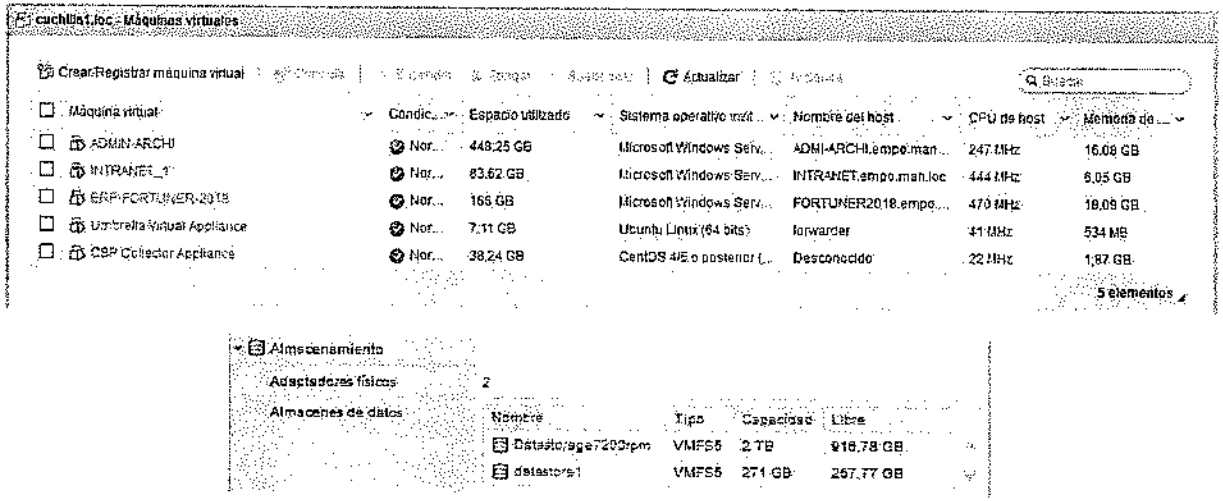
Data & Service

empocaldas

Cuchilla 5



Cuchilla 1

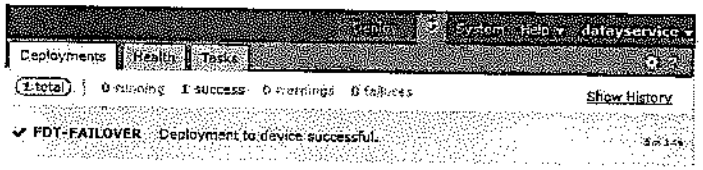


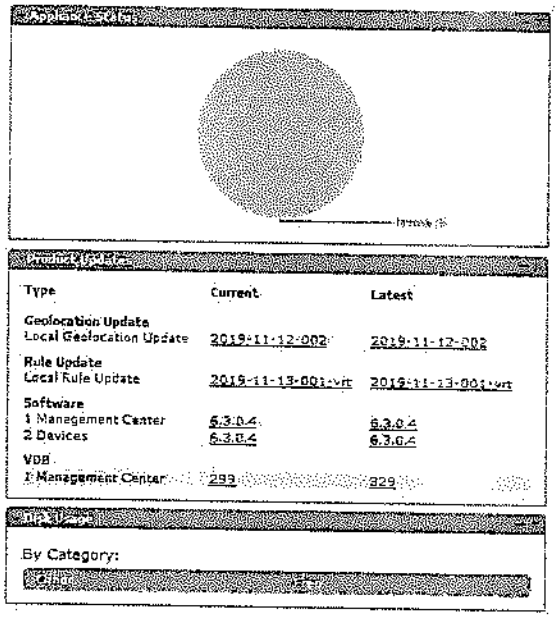
arcserve FORTINET KASPERSKY Windows Server Hyper-V Volbox

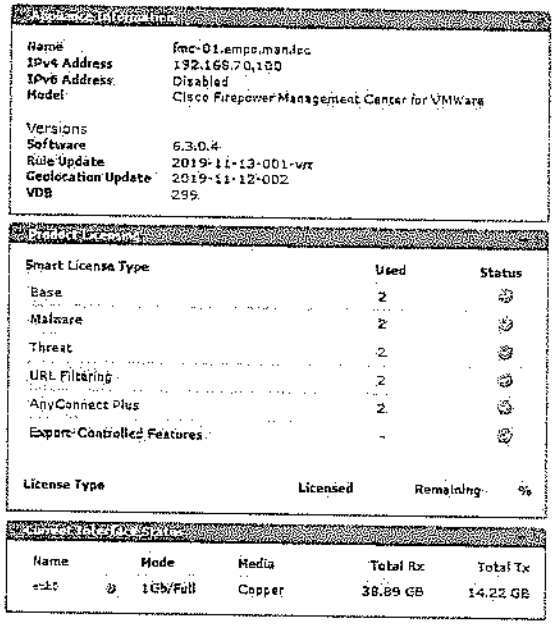
Data & Service

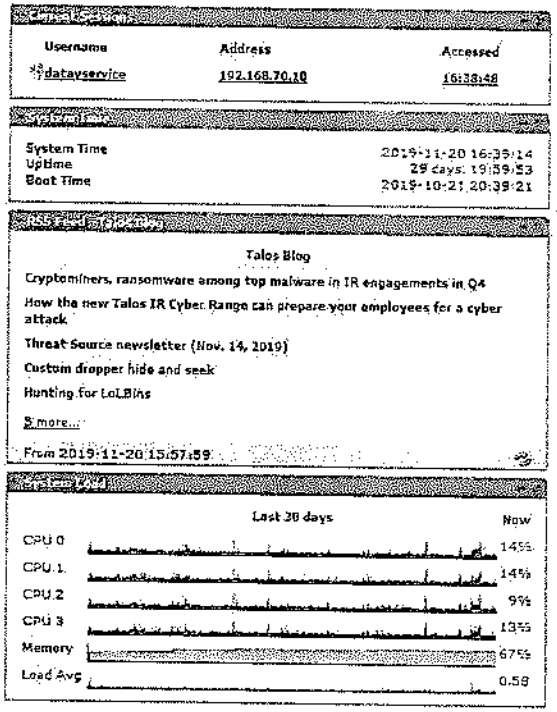
empocaldas

Estado del sistema Firewall







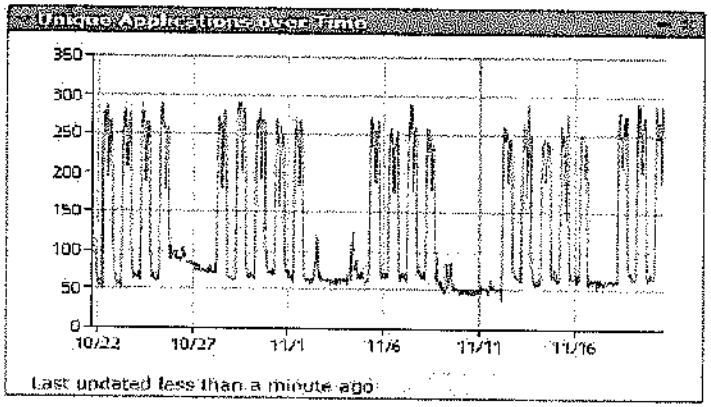


arcserve FORTINET KASPERSKY Windows Server Hyper-V Veeam

Data & Service

empocaldas

Flujo de tráfico durante el mes de Agosto



Aplicaciones arriesgadas con baja relevancia comercial

Risky Applications with Low Business Relevance

Application	Total Connections
TeamViewer	504,714
Facebook	151,853
YouTube	37,641
BitTorrent	26,567
Freenet	3,910
TuneIn	3,077
WeTransfer	2,881
MoPub	1,622
Skype File Transfer	1,473
QQ	1,332

Last updated 1 minute ago

NOTA: *Se han identificado las siguientes aplicaciones con alto consumo de ancho de banda, algunas de las aplicaciones relacionadas a continuación no son de uso empresarial, por lo cual deberían ser bloqueadas inmediatamente en todas las redes de la compañía. Se debe tener un mejor control de la red de visitantes, ya que, aunque es una red libre, el tráfico está saliendo por el mismo canal de la red corporativa lo cual consume el canal y la red se vuelve lenta.*

Application	Total Bytes (KB)
Sharepoint Online	965,706,273.25
DCE/RPC	374,927,192.80
Microsoft	117,851,966.42
Office 365	53,430,112.53
Microsoft Update	30,590,988.66
BITS	25,906,954.92
Google Play	18,181,522.89
Exchange Online	13,533,572.16
Amazon Web Services	13,275,036.35
Akamai	13,077,519.94
Facebook	12,352,045.67
Cisco	12,277,658.43
Eset	12,273,891.16
Sourcefire.com	11,714,624.69
YouTube	11,531,854.69

Last updated 1 minute ago

Application	Total Bytes (KB)
DCE/RPC	374,927,192.80
BITS	25,906,954.92
BOP	16,853,872.61
Amazon Web Services	13,275,036.35
Facebook	12,352,045.67
Eset	12,273,891.16
YouTube	11,531,854.69
Chrome	11,278,557.54
Firefox	10,192,200.24
Apple	7,153,402.09
Windows Update	5,975,498.02
Instagram	5,388,417.49
iTunes	4,773,731.04
iTunes Desktop	3,922,651.80
SMTP	3,147,861.86

Last updated less than a minute ago

Cisco Meraki · arcserve · FORTINET · KASPERSKY · Windows Server Hyper-V · Volbox

Data & Service

empocaldas

APLICACIONES CON ALTO RIESGO Y BAJA RELACIÓN CON EL NEGOCIO

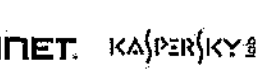
Algunas aplicaciones conllevan un alto riesgo porque pueden ser vectores de malware en la organización, poseer vulnerabilidades recientes, utilizar recursos de red sustanciales u ocultar las actividades de los atacantes. Otras aplicaciones tienen poca relevancia comercial: no son relevantes para las actividades de una organización típica. Cuando una aplicación tiene alto riesgo y baja relevancia comercial, es un buen candidato para el control de la aplicación para reducir el riesgo de su aplicación. Debe investigar estas aplicaciones para determinar si son importantes para controlar.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MB)
Gnutella	116	Very High	Very Low	0.08
BitTorrent	39	Very High	Very Low	3.24
Manolito	6	Very High	Very Low	0.01
Manolito client	6	Very High	Very Low	0.01
MyWay	2	Very High	Very Low	0.02

VERSIONES PELIGROSAS DEL NAVEGADOR WEB

Un perfil de su red reveló los siguientes viejos navegadores web en uso. Los navegadores web obsoletos son un vector importante para el malware de red y es importante actualizarlos (o animar a los usuarios). Estos navegadores a menudo tienen vulnerabilidades no parcheadas o conllevan otros riesgos.

BROWSER	VERSION	NUMBER OF HOSTS
Internet Explorer	10.0	2
Google Chrome	31.0.1650.57	2
Safari	12.1.2	2
Firefox	23.0	6

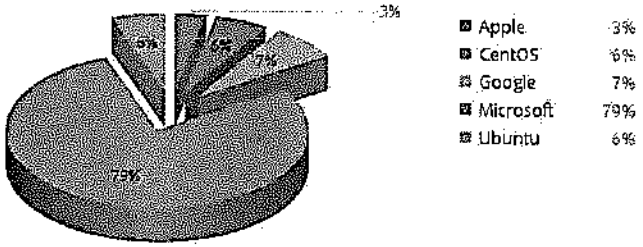


Data & Service

empocaldas

LOS DISPOSITIVOS MÓVILES EN SU RED

Los siguientes dispositivos móviles fueron perfilados en su red. Los dispositivos móviles pueden ser vulnerables, especialmente las versiones antiguas o con jailbreak. Es importante conocer cómo se utilizan los dispositivos móviles y establecer las políticas de seguridad adecuadas.



NAVEGACIÓN WEB RIESGOSA

Se identificaron las siguientes comunicaciones web que corresponden a la actividad de riesgo. Los sitios de malware, los proxies y anonimizadores abiertos, los registradores de pulsaciones de teclas, los sitios de phishing y las fuentes de spam son todas actividades de la Web que pueden poner en riesgo sus redes. Es aconsejable evaluar el uso de las tecnologías de filtrado de URL para detectar y controlar las comunicaciones a los sitios de riesgo.

URL CATEGORY	CONNECTIONS	BLOCKED	DATA INBOUND (KB)	DATA OUTBOUND (KB)
Social Network	130,047	149,453	13,374,828.42	885,893.41
Adult and Pornography	0	979	98.04	595.61
Cheating	0	3	0.19	2.75
Hacking	0	27	1.74	17.83
Malware Sites	0	265	16.98	180.12
Peer to Peer	0	1,087	68.97	531.60
Phishing and Other Frauds	0	9,759	697.99	4,172.47
Proxy Avoid and Anonymizers	0	1,340	88.93	666.54
SPAM URLs	0	2,113	138.68	1,477.93
Spyware and Adware	0	1,450	123.43	1,027.17

Data & Service

empocaldas

LOS ARCHIVOS QUE TRASLADAN SU RED

Downloads

FILE CATEGORY	FILE TYPE	PROTOCOL	COUNT
Archive	MSCAB	HTTP	42,045
Executables	MSEXE	HTTP	7,420
Archive	RAR	HTTP	3,580
PDF files	PDF	HTTP	1,502
Archive	ZIP	HTTP	374

Uploads

FILE CATEGORY	FILE TYPE	PROTOCOL	COUNT
PDF files	PDF	HTTP	382
Archive	GZ	HTTP	39
Office Documents	WRI	HTTP	39
Archive	ZIP	HTTP	20
Office Documents	MDI	HTTP	12

Misc

FILE CATEGORY	FILE TYPE	PROTOCOL	COUNT
Executables	MSEXE	NetBIOS-ssn (SMB)	4,176
Office Documents	NEW_OFFICE	FTP Data	3,024
PDF files	PDF	FTP Data	1,684
Office Documents	NEW_OFFICE	NetBIOS-ssn (SMB)	669
Executables	MSOLE2	FTP Data	63

arcserve FORTINET KASPERSKY Windows Server Hyper-V Valbox

Data & Service

empocaldas

Wireless Controller

Actualmente se tienen 3 redes WIFI en la compañía que funcionan de la siguiente manera:

1. La red **EMP_CORP**, es la red corporativa de la compañía la cual tiene un sistema de autenticación por Contraseña y MAC, todos los dispositivos que se deseen conectar a la red deben tener la autenticación de 2 factores.
2. La red **EMPO-VISITANTES**, es la red controlada por la usuaria Claudia Candamil para las personas externas a la compañía, la cual tiene un sistema de conexión por medio de portal cautivo, solo la persona que se encuentre registrada en el portal se conectara a la red indicada.
3. La red **EMPO-SISTEMAS**, es la red del área de T.I con la cual se relacionan los servicios de la compañía y se mantiene la comunicación entre los empleados de dicha área.

Controller Summary

Management IP Address	192.168.[illegible].4 , ::/128
Software Version	8.3.143.0
Field Recovery Image Version	7.6.101.1
System Name	WLC_Empocaldas
Up Time	27 days, 0 hours, 57 minutes
System Time	Wed Sep 11 16:57:23 2019
Redundancy Mode	N/A
Internal Temperature	+37 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	EMPOCALDAS
CPU(s) Usage	1%
Individual CPU Usage	0%/1%, 3%/1%
Memory Usage	38%
Fan Status	4200 rpm

Rogue Summary

Active Rogue APs	43	Detail
Active Rogue Clients	1	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

Session Timeout

Top WLANs

Profile Name	# of Clients	
EMP_CORP	17	Detail
EMPO-VISITANTES	16	Detail
EMPO-SISTEMAS	6	Detail

NOTA: *No se tiene un control adecuado de la red visitantes, ya que muchas personas se conectan a dicha red con fines de visitar redes sociales, youtube, entre otras cosas, dicha red debería utilizarse solo para usuarios visitantes.*

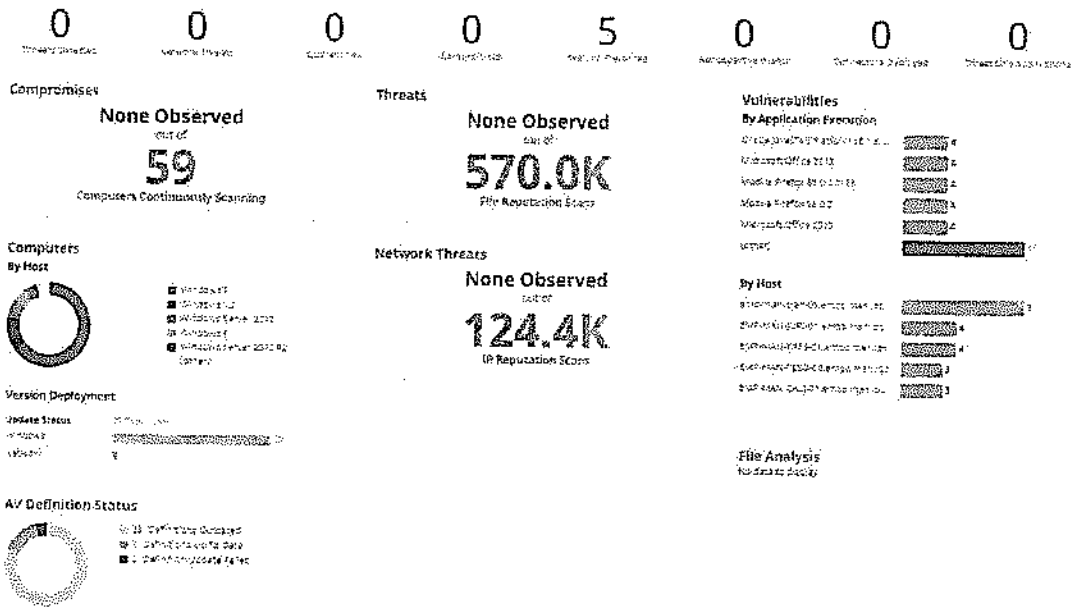
- *Es de recordar que las redes WIFI se deben utilizar con fines empresariales, debido a que su uso influye en la velocidad de transferencia de los datos de los usuarios de la compañía.*

cisco Small Business 220 Series · arcserve · FORTINET · KASPERSKY · Windows Server Hyper-V · Volbox

Data & Service

empocaldas

Advance Malware Protection ***(AMP)***

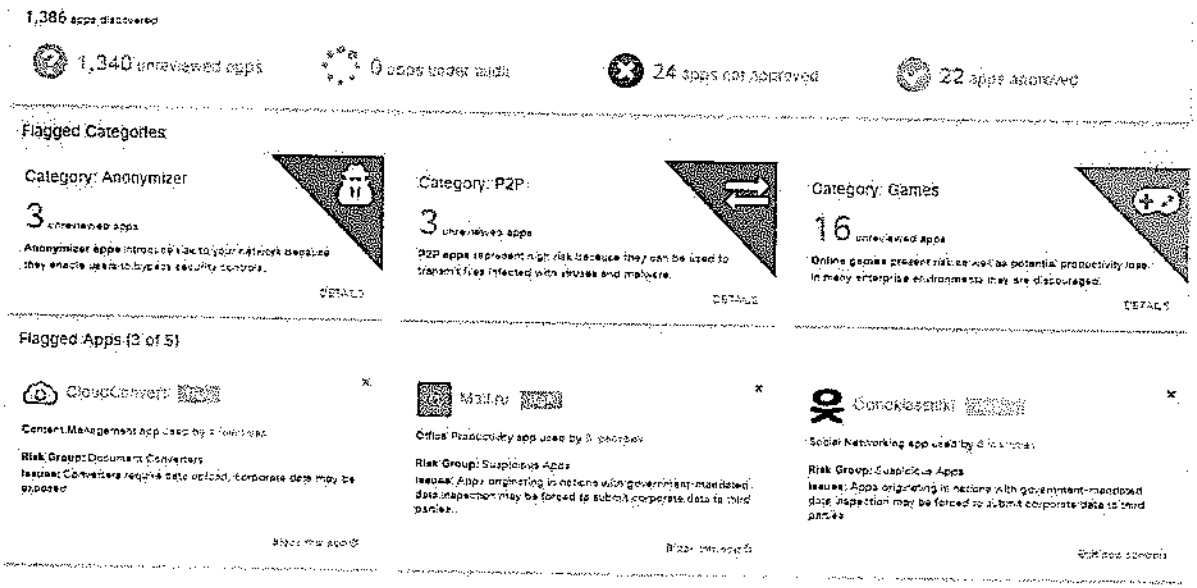


En los últimos 30 días la inteligencia global de amenazas a correlacionado diferentes tipos de archivos en los cuales no ha identificado comportamientos inadecuados, ni catalogados como Malware.

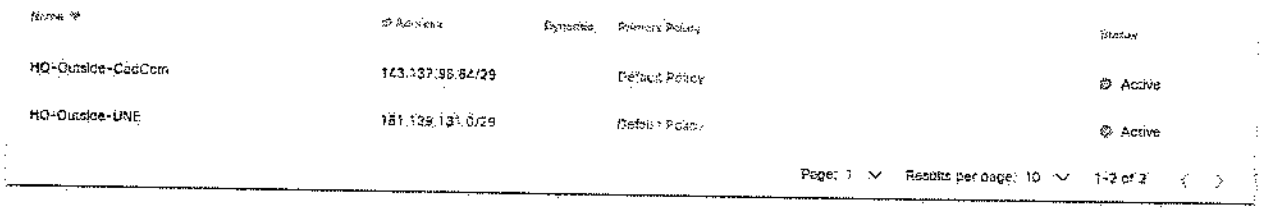
cisco Partner · arcserve · FORTINET · KASPERSKY · Windows Server Hyper-V · Veeam

Cisco Umbrella

*Se han bloqueado **782** solicitudes DNS las cuales se han categorizado como Malware, phishing y CnC.*



Umbrella es una solución basada en la nube diseñada para la protección de los dispositivos que están tanto dentro como fuera de la red corporativa.



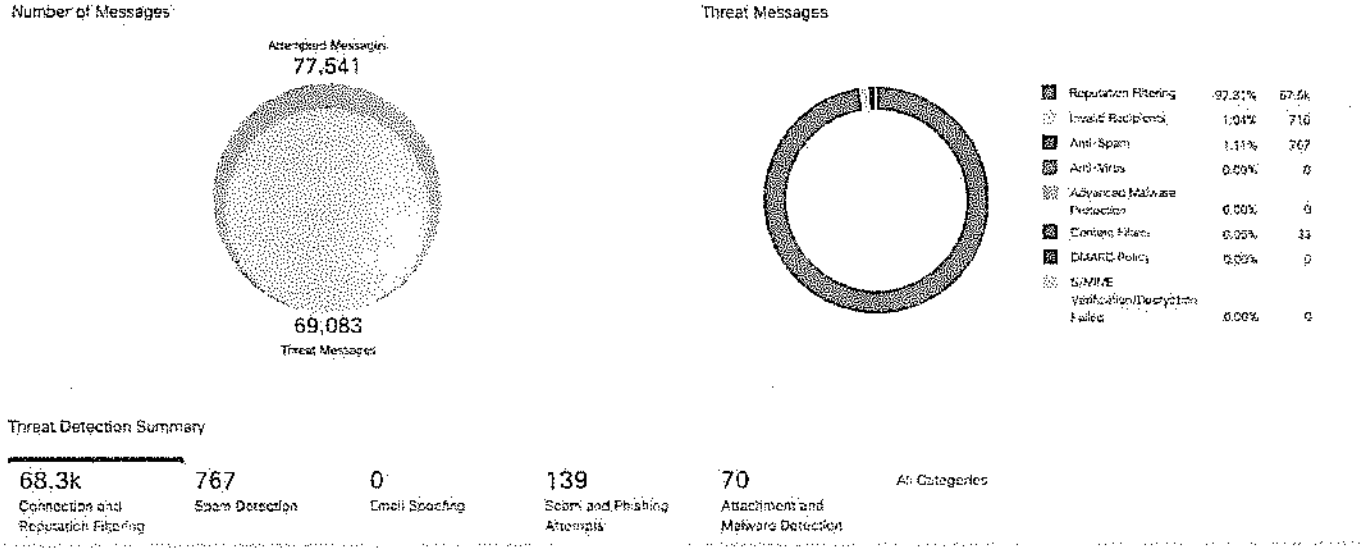
Umbrella** es un servicio pensado para proveer de acceso seguro a todos los usuarios, usen o no usen **VPN**, y proteger los datos sensibles que haya en las aplicaciones que utilicen. **(En el momento se están protegiendo 120 usuarios por medio de Roaming)

Data & Service

empocaldas

*Protección de correo electrónico en la nube **(Cloud Email Security)***

CES es su defensa contra la suplantación de identidad, los riesgos de correo electrónico comercial y el ransomware. Obtenga actualizaciones de inteligencia de amenazas cada tres a cinco minutos a través de Cisco Talos para contar con la protección más actualizada. Cisco Advanced Malware Protection protege contra malware furtivo en adjuntos y la inteligencia de URL líder en el sector combate enlaces maliciosos. Cisco Email Security también aumenta la seguridad de correo electrónico Office 365.



Proteger a nuestros usuarios contra amenazas de correo electrónico ahora es más fácil, con la herramienta CES veremos cómo las múltiples capas de seguridad mantienen a los atacantes alejados de las bandejas de entrada de nuestros correos.

- ***Se han obtenido 77.541 peticiones de correo electrónico que de acuerdo con el filtro de Malware y Ransomware, 69.083 han sido categorizados como altamente peligrosos.***
- ***Se han detenido el 92.81% de peticiones de acuerdo con el filtrado de reputación de CES.***

cisco Gold Partner · arcserve · FORTINET · KASPERSKY · Windows Server Hyper-V · Veeam

Data & Service

empocaldas

Tareas

Como es costumbre se envían las tareas que se realizaron en el mes de octubre y las que quedaron pendientes del presente mes. Se debe tener en cuenta que se tienen previstos controles de cambios en los aplicativos instalados en la compañía, ya que hay que afinar su comportamiento y funcionalidades, con relación a las necesidades de la compañía.

1. *Revisar los diferentes equipos en los cuales se han identificado problemas de seguridad, determinando que el antivirus este correctamente instalado, actualizado y activo.* ***(Empocaldas)***

Para recordar: Algunos malware se esconden en archivos que no son reconocidos para el sistema de Antivirus o el mismo firewall como maliciosos ya el nombre no deja a la vista una amenaza, el sistema de Empocaldas contiene un sistema de Sandbox el cual analiza los flujos de archivos y comportamientos, si el archivo comienza a efectuar cargas del equipos altas, o a bajar información de internet son comportamientos que los Antivirus locales no lograrían identificar, es por esto que se toma el lapso de hasta 30 minutos para entender el firewall que es una amenaza posible y la bloquea sin dejarlo pasar hacia la LAN.

2. *En el mes de agosto se ajustaron algunas configuraciones de seguridad del software y Hardware que se instalaron en la compañía entre los cuales están:*

- *Mejora de políticas en el Módulo FIREPOWER Versión: 6.3.0.4* ***(Modulo de control de aplicaciones)***
  - *Se ajustaron las reglas de QoS.*
- *Mejora en parámetros del Módulo AMP* ***(Modulo de protección avanzada de Malware)***
  - *Se aplicaron filtro avanzados contra Malware.*
  - *Se cambiaron los equipos de modo Audit a modo protect*
- *Mejora en las políticas del Módulo UMBRELLA* ***(Modulo de protección DNS)***
  - *Se afinaron las políticas de VPN desde las seccionales hacia la sede principal.*
- *Mejora de herramienta Cloud Email Security* ***(Protección de correo electrónico en la nube)***
  - *Se aplicaron filtros avanzados de malware phishing y CnC.*
- *Se implemento el nuevo sistema de backup Versión 7 Actualización 1* ***(Arcserve UDP - ASBU)***

3. *Para mejorar el ancho de banda de las redes WiFi, la red de Visitante está saliendo por el canal de respaldo para que no se vea afectado el tráfico corporativo.*

cisco Gold Partner · arcserve · FORTINET · KASPERSKY · Windows Server · Volbox