	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	0030/2017	Acta N°	11 Y FINAL	1. VALOR INICIAL (incluido IVA)	48,880,000
				2. VALOR ADICIÓN (+)	
CONTRATISTA	DATA & SERVICE			3. VALOR TOTAL (1+2)	48,880,000
NIT O CC:	810001025-7			4. VALOR ACTAS ANTERIORES (-)	40,733,000
CDP (#, rubro y fecha)	00103 DE ENERO 02 DE 2017			5. VALOR PRESENTE ACTA (-)	8,147,000
RP (#, rubro y fecha)	00102 DEL 02 DE ENERO DE 2017			6. VALOR NO EJECUTADO (3 - 4 - 5)	0

OBJETO DEL CONTRATO: 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.

TIPO DE RECURSOS		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.

Saidy Gaviria A. — NOMBRE DE QUIEN RECIBE

18. Dic- 2017. — 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: 13 DE DICIEMBRE DE 2017

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

DATOS PARA LA TRANSFERENCIA DE PAGOS		
CORRIENTE	05902062602	BANCOLOMBIA
CUENTA	TIPO DE CUENTA	BANCO

Data & Service

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 once (11) días del mes de Diciembre (12) del año dos mil diecisiete (2017).

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.: 000012036

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

FECHA: 2017/12/11

IVA REGIMEN COMÚN

Presente su factura
Para hacer efectiva
su garantía.

Informacion@datayservice.com

Resolución N° 100000091578 del 13 de Abril de 2016 Rango de aprobación 11750 al 16000

Información del Cliente:

NOMBRE : EMPOCALDAS S.A. E.S.P
DIRECCION: CRA. 23 NRO. 75-82
CIUDAD : MANIZALES
VENDEDOR : 00

NIT/CC : 890803239
TEL/FAX: 8867080

VENCE : 2017 12 26

UNIDADES	DESCRIPCION	VALOR UNITARIO	VALOR NETO
1	SERVICIOS PARA ADMINISTRAR,	6,846,218.00	6,846,218.00
1	OPTIMIZAR, ASEGURAR Y DAR SOPO	0.00	0.00
1	A LOS RECURSOS DEL CENTRO DE	0.00	0.00
1	DATOS, SISTEMAS DE SEGURIDAD	0.00	0.00
1	INFORMÁTICA, BACKUP Y RESTAURA	0.00	0.00

Observaciones

DATA & SERVICE LTDA
Nit: 810.001.025-7
Tel: 88 12 77

SEGUN CONTRATO No. 0030-2017

FIRMA Y SELLO ALMACÉN

Recibido

Firma Documento o Sello

SUBTOTAL	$	6,846,218.00
DESCUENTO	$	0.00
IVA	$	1,300,782.00
TOTAL	$	8,147,000.00

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.

ACTA DE RECIBO # 11 Y FINAL

CONTRATO	No. 0030/2017
OBJETO	PRESTACION DE SERVICIOS PROFESIONALES PARA ADMINISTRAR, OPTIMIZAR, ASEGURAR Y DAR SOPORTE A LOS RECURSOS DEL CENTRO DE CÓMPUTO, RED DE DATOS, SISTEMAS DE SEGURIDAD INFORMATICA, DE BACKUP Y RESTAURACIÓN.
CONTRATISTA	DATA & SERVICE LTDA
VALOR CONTRATO	$48.880.000 IVA INCLUIDO
RECURSOS	PROPIOS

En la ciudad de Manizales a los trece (13) días del mes de diciembre de 2017, se reunieron JOHN JAIRO GIRALDO VILLA, Jefe Sección 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, como contratista, con el fin de realizar el Acta de Recibo No. 11 y final al Contrato No. 0030 de 2017.

VALOR CONTRATO	$48,880,000.00
ACTA # 1	$4,073,300.00
ACTA # 2	$4,073,300.00
ACTA # 3	$4,073,300.00
ACTA # 4	$4,073,300.00
ACTA # 5	$4,073,300.00
ACTA # 6	$4,073,300.00
ACTA # 7	$4,073,300.00
ACTA # 8	$4,073,300.00
ACTA # 9	$4,073,300.00
ACTA # 10	$4,073,300.00
ACTA # 11 Y FINAL	$8,147,000.00
VALOR EJECUTADO	$48,880,000.00
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

Preparó: Maria del Carmen Guzman

INFORME DE SUPERVISION

CONTRATO	Nº 0030/2017
CONTRATISTA	DATA & SERVICE LTDA
OBJETO	PRESTACION DE SERVICIOS PROFESIONALES PARA ADMINISTRAR, OPTIMIZAR, ASEGURAR Y DAR SOPORTE A LOS RECURSOS DEL CENTRO DE CÓMPUTO. RED DE DATOS, SISTEMAS DE SEGURIDAD INFORMATICA, DE BACKUP Y RESTAURACIÓN
VALOR	$48.880.000 IVA INCLUIDO
RECURSOS	EMPOCALDAS S.A E.S.P

En cumplimiento del contrato 0030 de 2017, cuyo objeto es PRESTACION DE SERVICIOS PROFESIONALES PARA ADMINISTRAR, OPTIMIZAR, ASEGURAR Y DAR SOPORTE A LOS RECURSOS DEL CENTRO DE CÓMPUTO. RED DE DATOS, SISTEMAS DE SEGURIDAD INFORMATICA, DE BACKUP Y RESTAURACIÓN, se evidenció que dicho contrato se desarrolló satisfactoriamente a los términos y especificaciones del contrato según el objeto contractual mencionado.

VALOR CONTRATO	$48,880,000.00
ACTA # 1	$4,073,300.00
ACTA # 2	$4,073,300.00
ACTA # 3	$4,073,300.00
ACTA # 4	$4,073,300.00
ACTA # 5	$4,073,300.00
ACTA # 6	$4,073,300.00
ACTA # 7	$4,073,300.00
ACTA # 8	$4,073,300.00
ACTA # 9	$4,073,300.00
ACTA # 10	$4,073,300.00
ACTA # 11 Y FINAL	$8,147,000.00
VALOR EJECUTADO	$48,880,000.00
VALOR POR EJECUTAR	$0.00

Manizales, 13 de diciembre de 2017

JOHN JAIRO GIRALDO VILLA
Jefe Sección Sistemas

Preparó: María del Carmen Guzman Quintero

Data & Service

Manizales, diciembre 5 del 2017

Señores
EMPOCALDAS
Atn. Ing. John Jairo Jaramillo.
Sistemas

Asunto: INFORME ESTADO INFRAESTRUCTURA PERIODO NOVIEMBRE

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 - 192.168.70.12
ii. Vmware 6 – 192.168.70.13
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 - 192.168.70.15

Soporte plataforma de Seguridad perimetral cisco con los siguientes componentes:

Firewall Físico Cisco ASA5515 con módulo firepower - 192.168.1.1

Firewall de Aplicaciones SourceFire Manager – 192.168.70.9

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

Jonathan Rodriguez Paipa
Director de proyectos

Data & Service

SISTEMA DE BACKUP

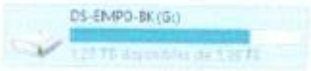
Detalles en general

Con respecto al sistema de Arcserve la data_store se encuentra con una disponibilidad por el momento para soportar la operación de retención del backup, el detalle del consumo y disponibilidad del almacenamiento sería el siguiente:

1. Respaldamos 10.3 TB de producción y se comprimen hasta 5.22 TB

Nombre	Recuento de planes	Datos protegidos	Deduplicación	Compresión	Reducción de datos general	Espacio ocupado
usuario-a2ar7d3.empo.mx\ac						
DS-EMPO-BK	4	10.3 TB	N/D	49%	49%	5.22 TB

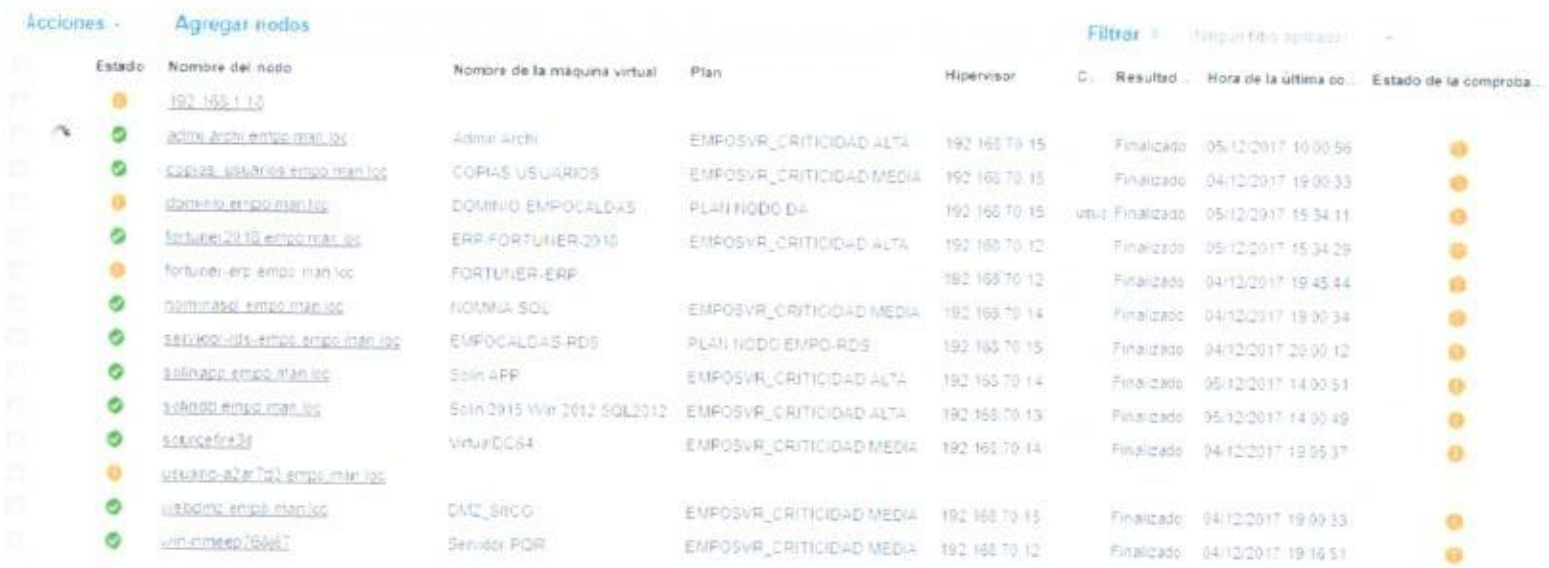
2. Dentro del data_store el cual está ubicado dentro del servidor 192.168.1.18 el estado el siguiente:



Cisco Select Partner · arcserve · FORTINET · KASPERSKY · Windows Server · Volbox

Data & Service

Lista de servidores protegidos actualmente


Acciones · Agregar nodos Filtrar

Estado	Nombre del nodo	Nombre de la máquina virtual	Plan	Hipervisor	C..	Resultad..	Hora de la última co..	Estado de la comproba..
	192.168.1.10							
	admi-archi.empo.man.loc	Admin Archi	EMPOSVR_CRITICIDAD ALTA	192.168.70.15		Finalizado	05/12/2017 10:00:56	
	copias_usuarios.empo.man.loc	COPIAS USUARIOS	EMPOSVR_CRITICIDAD MEDIA	192.168.70.15		Finalizado	04/12/2017 19:00:33	
	dominio.empo.man.loc	DOMINIO EMPOCALDAS	PLAN NODO DA	192.168.70.15	virtu	Finalizado	05/12/2017 15:34:11	
	fortuner2018.empo.man.loc	ERP FORTUNER 2018	EMPOSVR_CRITICIDAD ALTA	192.168.70.12		Finalizado	05/12/2017 15:34:29	
	fortuner-erp.empo.man.loc	FORTUNER-ERP		192.168.70.12		Finalizado	04/12/2017 19:45:44	
	nominasql.empo.man.loc	NOMINA SQL	EMPOSVR_CRITICIDAD MEDIA	192.168.70.14		Finalizado	04/12/2017 19:00:34	
	servicio-rds-empo.empo.man.loc	EMPOCALDAS RDS	PLAN NODO EMPO-RDS	192.168.70.15		Finalizado	04/12/2017 20:00:12	
	solinapp.empo.man.loc	Solin APP	EMPOSVR_CRITICIDAD ALTA	192.168.70.14		Finalizado	05/12/2017 14:00:51	
	solinsql.empo.man.loc	Solin 2015 Win 2012 SQL2012	EMPOSVR_CRITICIDAD ALTA	192.168.70.13		Finalizado	05/12/2017 14:00:49	
	sourcefire3d	VirtualDC64	EMPOSVR_CRITICIDAD MEDIA	192.168.70.14		Finalizado	04/12/2017 19:05:37	
	usuario-a2ar7q3.empo.man.loc							
	usbpmz.empo.man.loc	DMZ_SIRCO	EMPOSVR_CRITICIDAD MEDIA	192.168.70.15		Finalizado	04/12/2017 19:00:33	
	vm-mweb7bbk7	Servidor POR	EMPOSVR_CRITICIDAD MEDIA	192.168.70.12		Finalizado	04/12/2017 19:16:51	

Notas:

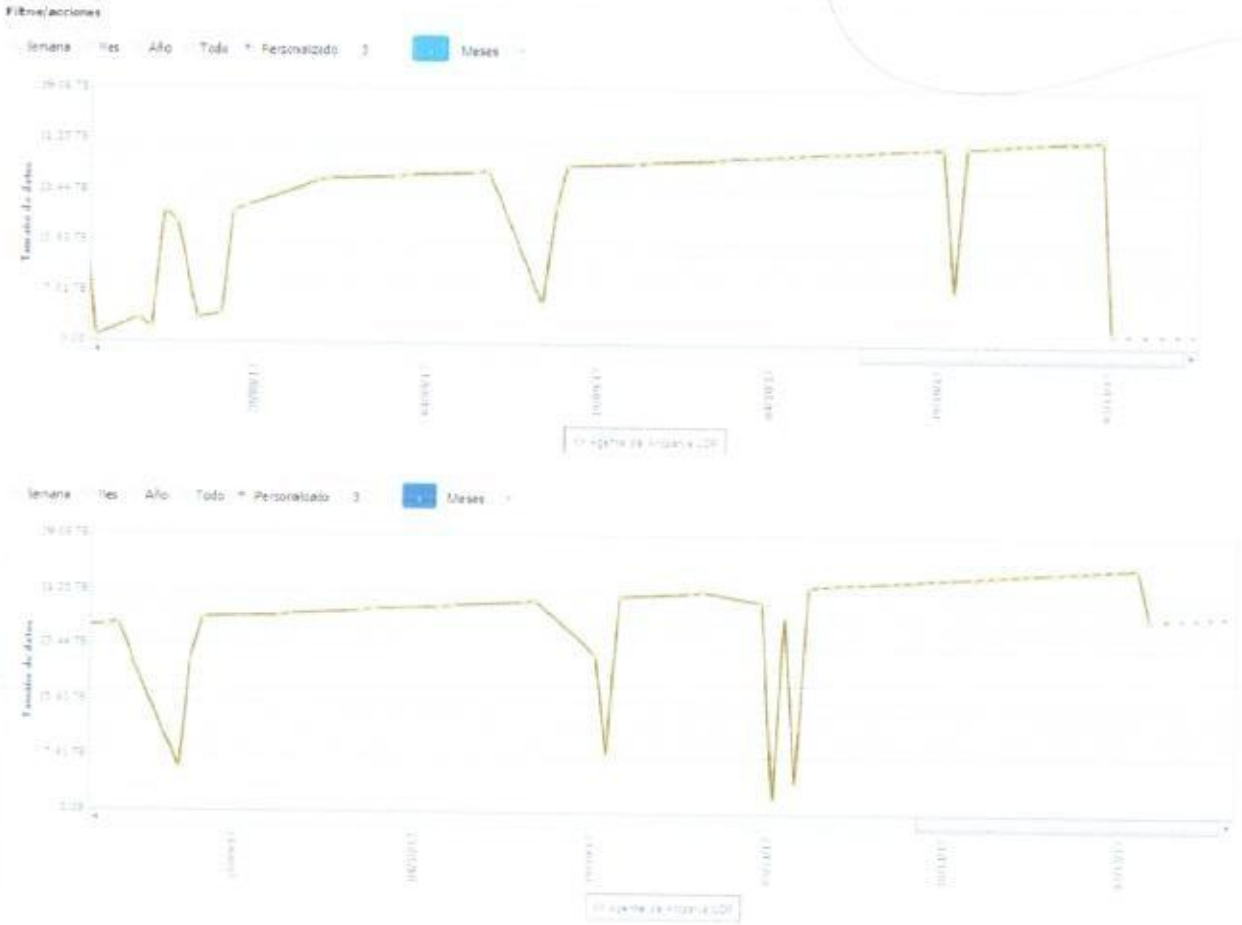
1. Se ha dejado de proteger el servidor llamado **fortuner-erp.empo.man.loc** el cual ha sido reemplazado por fortuner2018.empo.man.loc
2. El backup del servidor **fortuner-erp.empo.man.loc** quedara alojado por un tiempo, mientras se normaliza la operación del nuevo servidor.

Recomendaciones:

1. Aumento del Data_store de backup: podríamos utilizar una partición dentro del server 192.168.1.18 la cual se identifica como E:\ la cua tiene aproximadamente 3 TB que nos servirían como respaldo.

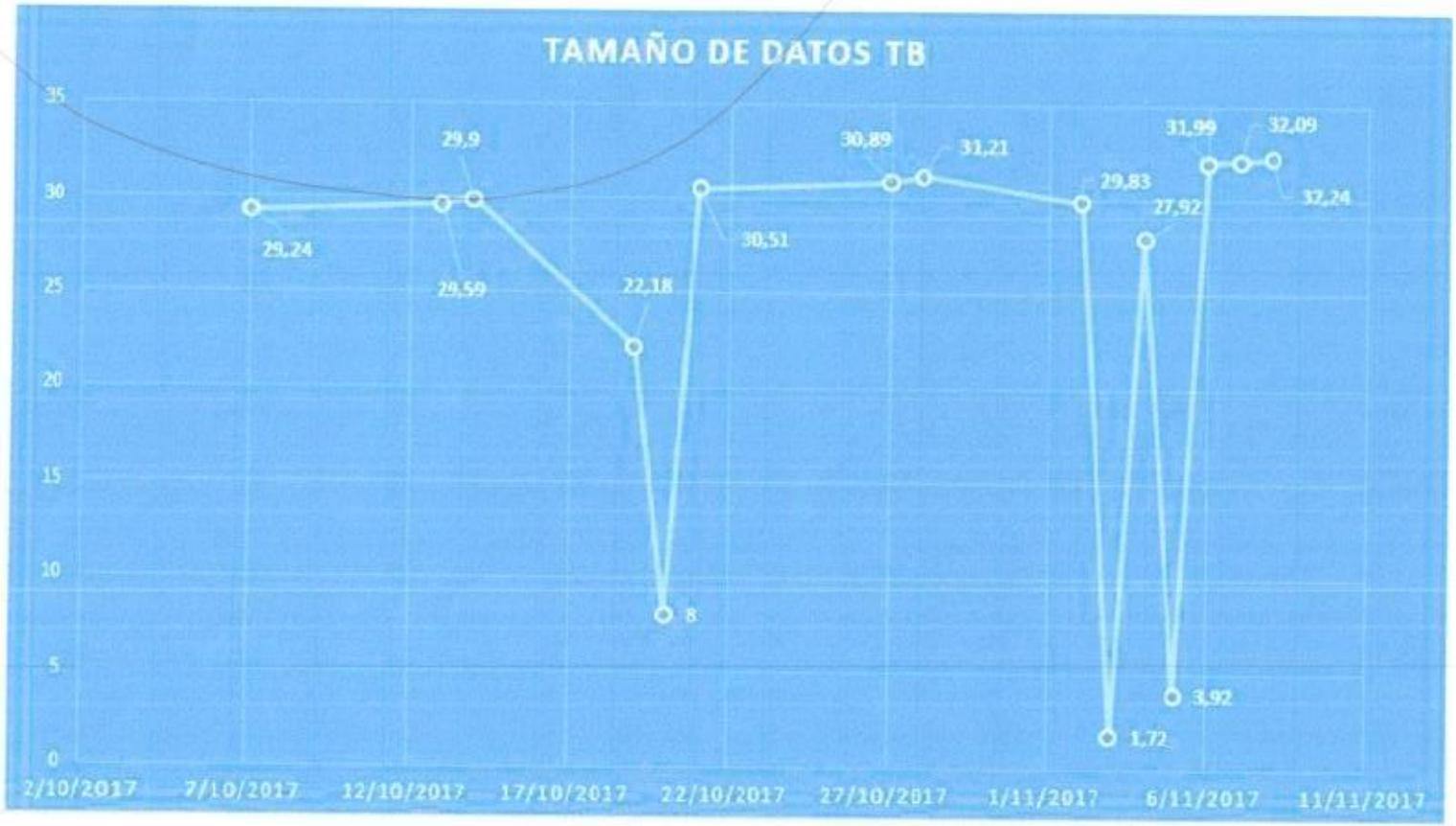
Data & Service

Tendencia de Backup durante los últimos tres (3) meses



Data & Service

Tendencia de backup de los dos últimos meses :



Data & Service

Tendencia de backup del ultimo mes:

Data & Service

Backup de Cintas

Inventario de cintas disponibles

Name	Tape Name
<Slot: 1> <2200460> F-D2D-MON-04/12/17	F-D2D-MON-04/12/17
<Slot: 2> <2200461> F-D2D-MON-04/12/17	F-D2D-MON-04/12/17
<Slot: 3> <2200462> F-D2D-MON-04/12/17	F-D2D-MON-04/12/17
<Slot: 4> <N/A> <Blank Media>	*
<Slot: 5> <2200446> F-D2D-TUE-21/11/17	F-D2D-TUE-21/11/17
<Slot: 6> <2200447> F-D2D-TUE-21/11/17	F-D2D-TUE-21/11/17
<Slot: 7> <2200448> F-D2D-TUE-21/11/17	F-D2D-TUE-21/11/17
<Slot: 8> <N/A> <Empty>	*
<Slot: 9> <2200449> F-D2D-TUE-21/11/17	F-D2D-TUE-21/11/17
<Slot: 10> <N/A> <Blank Media>	*
<Slot: 11> <N/A> <Blank Media>	*
<Slot: 12> <N/A> <Blank Media>	*
<Slot: 13> <N/A> <Blank Media>	*
<Slot: 14> <N/A> <Blank Media>	*
<Slot: 15> <N/A> <Blank Media>	*
<Slot: 16> <N/A> <Blank Media>	*
<Slot: 17> <N/A> <Blank Media>	*
<Slot: 18> <N/A> <Blank Media>	*
<Slot: 19> <N/A> <Blank Media>	*
<Slot: 20> <N/A> <Blank Media>	*
<Slot: 21> <N/A> <Blank Media>	*
<Slot: 22> <N/A> <Blank Media>	*
<Slot: 23> <N/A> <Cleaning Tape>	*
IBM ULT3580-HH5	

Tareas de backup a cintas

Group by: Job | Show history in last: 30 Days | Update

	Last Result	MB	Files	Missed	MB/Mi...	Time Used	Job ID
Backup UDP	122 job executions: 14 finished, 0 incomplete, 1 failed, 0 canceled, 1 active)						
2017-12-04 22:00:00	Active	N/A	N/A	N/A	N/A	23:16:40	2067
2017-12-03 22:00:00	Canceled	N/A	N/A	N/A	N/A	10:00:32	2064
2017-12-01 22:00:14	Finished	N/A	N/A	N/A	N/A	24:57:10	2060
2017-11-30 22:00:00	Finished	4,833,355	64,657	0	365.95	22:39:22	2057
2017-11-29 22:00:00	Finished	N/A	N/A	N/A	N/A	21:50:14	2054
2017-11-28 09:29:36	Finished	4,998,439	21,840	0	3571.78	23:10:29	2050
2017-11-27 22:00:00	Failed	N/A	N/A	N/A	N/A	09:56:28	2047
2017-11-26 22:00:14	Finished	4,920,966	37,996	0	2855.03	21:19:06	2044
2017-11-18 22:00:00	Canceled	N/A	N/A	N/A	N/A	09:19:46	2041
2017-11-18 22:00:00	Finished	N/A	N/A	N/A	N/A	21:23:27	2038
2017-11-17 22:00:00	Finished	N/A	N/A	N/A	N/A	21:23:34	2035
2017-11-16 22:00:00	Canceled	N/A	N/A	N/A	N/A	09:04:12	2032
2017-11-15 22:00:00	Canceled	N/A	N/A	N/A	N/A	10:47:15	2029
2017-11-14 22:00:14	Finished	4,816,022	64,133	0	3992.17	20:06:22	2026
2017-11-13 22:00:00	Canceled	N/A	N/A	N/A	N/A	24:45:22	2023
2017-11-11 22:00:00	Finished	N/A	N/A	N/A	N/A	19:28:32	2020
2017-11-10 22:00:00	Finished	N/A	N/A	N/A	N/A	20:15:32	2017
2017-11-09 22:00:00	Finished	N/A	N/A	N/A	N/A	19:17:16	2014
2017-11-08 22:00:00	Finished	N/A	N/A	N/A	N/A	19:39:08	2011
2017-11-07 22:00:14	Finished	4,754,855	72,632	0	4102.82	19:15:36	2008
2017-11-06 22:00:00	Canceled	N/A	N/A	N/A	N/A	11:06:24	2005
2017-11-05 22:00:00	Finished	N/A	N/A	N/A	N/A	10:16:26	2002

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

Data & Service

LOG del Backup a cintas:

- Week[19/11/2017 - 25/11/2017]
  - Job2067 (Database pruning job) [Finished] [SERVIDOR3630] (25/11/2017 12:00:00 - 25/11/2017 12:00:22) [Job No. 1]
  - Job2066 (Database pruning job) [Finished] [SERVIDOR3630] (24/11/2017 12:00:00 - 24/11/2017 12:00:22) [Job No. 1]
  - Job2065 (Database pruning job) [Finished] [SERVIDOR3630] (23/11/2017 12:00:00 - 23/11/2017 12:00:22) [Job No. 1]
  - Job2064 (Database pruning job) [Finished] [SERVIDOR3630] (22/11/2017 12:00:00 - 22/11/2017 12:00:26) [Job No. 1]
  - Job2062 (Backup_UDP) [Failed] [SERVIDOR3630] (21/11/2017 22:00:08 - 22/11/2017 07:56:36) [Job No. 2]
  - Job2061 (Database pruning job) [Finished] [SERVIDOR3630] (21/11/2017 12:00:04 - 21/11/2017 12:00:28) [Job No. 1]
  - Job2059 (Backup_UDP) [Finished] [SERVIDOR3630] (20/11/2017 22:00:14 - 21/11/2017 19:19:20) [Job No. 2]
  - Job2058 (Database pruning job) [Finished] [SERVIDOR3630] (20/11/2017 12:00:00 - 20/11/2017 12:00:22) [Job No. 1]
  - Job2056 (Backup_UDP) [Canceled] [SERVIDOR3630] (19/11/2017 23:00:10 - 20/11/2017 07:16:56) [Job No. 2]
  - Job2055 (Database pruning job) [Finished] [SERVIDOR3630] (19/11/2017 12:00:10 - 19/11/2017 12:00:32) [Job No. 1]
  - Generic Logs

- Week[26/11/2017 - 02/12/2017]
  - Job2082 (Database pruning job) [Finished] [SERVIDOR3630] (02/12/2017 12:00:06 - 02/12/2017 12:00:30) [Job No. 1]
  - Job2080 (Backup_UDP) [Finished] [SERVIDOR3630] (01/12/2017 22:00:14 - 02/12/2017 22:57:24) [Job No. 2]
  - Job2079 (Database pruning job) [Finished] [SERVIDOR3630] (01/12/2017 12:00:04 - 01/12/2017 12:00:26) [Job No. 1]
  - Job2077 (Backup_UDP) [Finished] [SERVIDOR3630] (30/11/2017 22:00:08 - 01/12/2017 20:39:30) [Job No. 2]
  - Job2076 (Database pruning job) [Finished] [SERVIDOR3630] (30/11/2017 12:00:04 - 30/11/2017 12:00:26) [Job No. 1]
  - Job2074 (Backup_UDP) [Finished] [SERVIDOR3630] (29/11/2017 22:00:08 - 30/11/2017 19:50:22) [Job No. 2]
  - Job2073 (Database pruning job) [Finished] [SERVIDOR3630] (29/11/2017 12:00:00 - 29/11/2017 12:00:22) [Job No. 1]
  - Job2072 (Database pruning job) [Finished] [SERVIDOR3630] (28/11/2017 12:00:02 - 28/11/2017 12:00:26) [Job No. 1]
  - Job2070 (Backup_UDP) [Finished] [SERVIDOR3630] (28/11/2017 09:20:50 - 29/11/2017 08:31:18) [Job No. 2]
  - Job2069 (Database pruning job) [Finished] [SERVIDOR3630] (27/11/2017 12:00:00 - 27/11/2017 12:00:22) [Job No. 1]
  - Job2068 (Database pruning job) [Finished] [SERVIDOR3630] (26/11/2017 12:00:02 - 26/11/2017 12:00:24) [Job No. 1]
  - Generic Logs

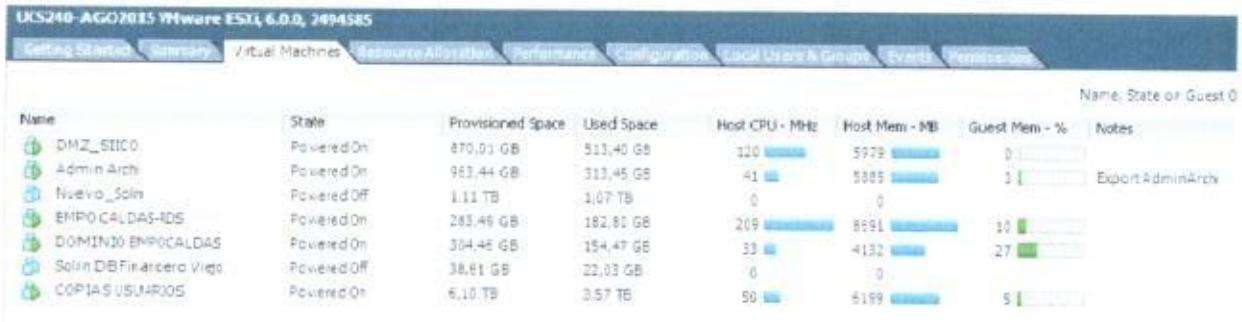
- This Week[03/12/2017 - 09/12/2017]
  - Job2089 (Database pruning job) [Finished] [SERVIDOR3630] (05/12/2017 12:00:52 - 05/12/2017 12:01:58) [Job No. 1]
  - Job2087 (Backup_UDP) [Active] [SERVIDOR3630] [Job No. 2]
  - Job2086 (Database pruning job) [Finished] [SERVIDOR3630] (04/12/2017 12:00:00 - 04/12/2017 12:00:24) [Job No. 1]
  - Job2084 (Backup_UDP) [Canceled] [SERVIDOR3630] (03/12/2017 22:00:06 - 04/12/2017 08:09:38) [Job No. 2]
  - Job2083 (Database pruning job) [Finished] [SERVIDOR3630] (03/12/2017 12:00:02 - 03/12/2017 12:00:24) [Job No. 1]
  - Generic Logs

Cisco Select Partner · arcserve · FORTINET · KASPERSKY · Windows Server · Volbox

Data & Service

Estado de los ambientes servidores

Servidor 192.168.70.15



Almacenamiento consumido dentro del Host 70.15

Cisco Select Partner · arcserve · FORTINET · KASPERSKY · Windows Server · Volbox

Data & Service

Servidor 192.168.70.14

BladeS VMware ESXi 5.5.0, 1331820

Getting Started | Summary | Virtual Machines | Resource Allocation | Performance | Configuration | Local Users & Groups | Events | Permissions

Na

Name	State	Provisioned Space	Used Space	Host CPU - MHz	Host Mem - MB	Guest Mem - %
VirtuaDC64	Powered On	523,48 GB	507,14 GB	4640	10295	15
NOD32	Powered Off	121,21 GB	120,00 GB	0	0	
Solin APP	Powered On	339,20 GB	339,20 GB	2433	13472	1
NOMINA SQL	Powered On	608,89 GB	413,46 GB	1261	4147	3
CANDADO FORTUNER	Powered Off	81,23 GB	80,00 GB	0	0	
INTRANET	Powered Off	104,21 GB	10,05 KB	0	0	

Almacenamiento consumido dentro del Host 70.14

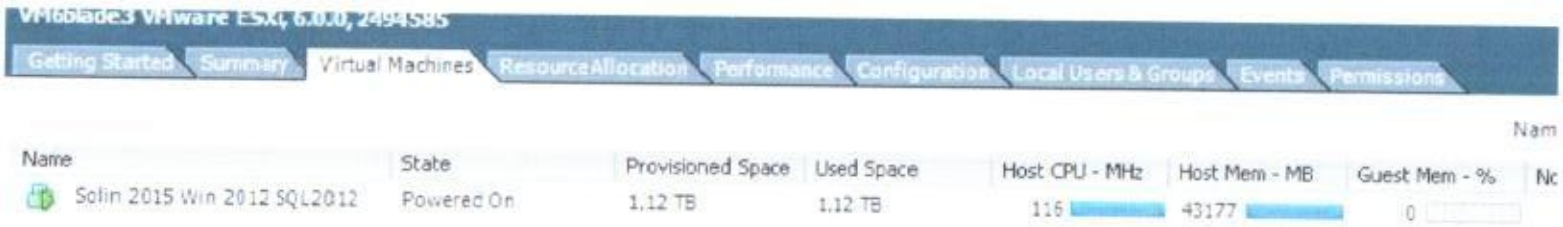
Datastores

Refresh | Delete | Add Storage... | R

Identification	Device	Drive Type	Capacity	Free	Type	Last Update	Hardware Acceleration
Datastorage7200L...	IBM Serial Attach...	Non-SSD	2,00 TB	341,97 GB	VMFS5	10/05/2017 10:16:36	Unknown
datastore1	LSI Serial Attach...	Non-SSD	271,00 GB	262,85 GB	VMFS5	10/05/2017 0:03:36	Unknown

Data & Service

Servidor 192.168.70.13



Name	State	Provisioned Space	Used Space	Host CPU - MHz	Host Mem - MB	Guest Mem - %
Solin 2015 Win 2012 SQL2012	Powered On	1,12 TB	1,12 TB	116	43177	0

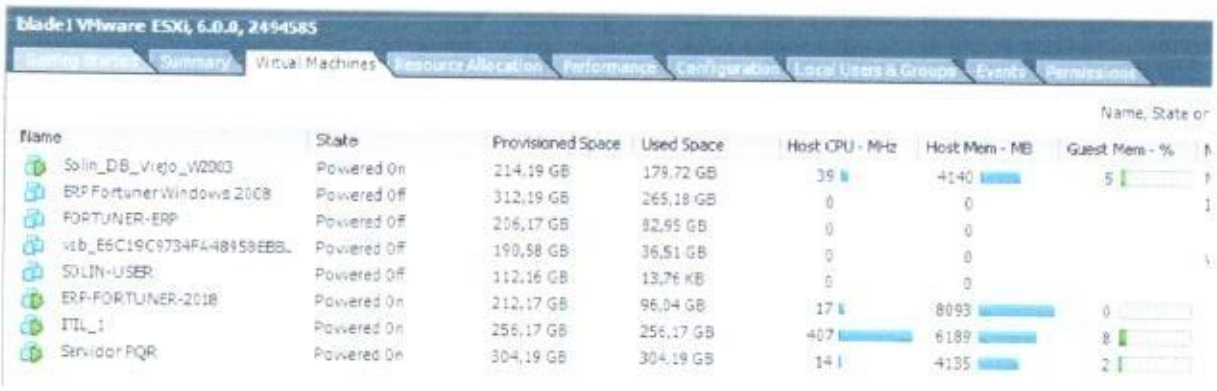
Almacenamiento consumido dentro del Host 70.13

Datastores

Refresh Delete Add Storage...

Identification	Device	Drive Type	Capacity	Free	Type	Last Update	Hardware Acceleration
DataStorage 7.2K...	IBM Serial Attach...	Non-SSD	999,75 GB	306,45 GB	VMFS5	04/11/2017 20:10:16	Not supported
datastore1	LSI Serial Attach...	Non-SSD	271,00 GB	261,88 GB	VMFS5	04/11/2017 20:10:16	Unknown
DataStore2 15 K	IBM Serial Attach...	Non-SSD	899,75 GB	399,96 GB	VMFS5	04/11/2017 20:10:16	Not supported
Files_4 ArdminArc...	IBM Serial Attach...	Non-SSD	899,75 GB	898,80 GB	VMFS5	04/11/2017 20:10:16	Unknown

Servidor 192.168.70.12



Name	State	Provisioned Space	Used Space	Host CPU - MHz	Host Mem - MB	Guest Mem - %
Solin_DB_Viejo_W2003	Powered On	214,19 GB	179,72 GB	39	4140	5
ERP Fortuner Windows 2008	Powered Off	312,19 GB	265,18 GB	0	0	
FORTUNER-ERP	Powered Off	206,17 GB	82,95 GB	0	0	
vib_E6C19C9734F448958EB8...	Powered Off	190,58 GB	36,51 GB	0	0	
SOLIN-USER	Powered Off	112,16 GB	13,76 KB	0	0	
ERP-FORTUNER-2018	Powered On	212,17 GB	96,04 GB	17	8093	0
ITIL_1	Powered On	256,17 GB	256,17 GB	407	6189	8
Servidor PQR	Powered On	304,19 GB	304,19 GB	141	4135	2

Data & Service

Almacenamiento consumido dentro del Host 70.12

Datastores

Refresh Delete

Identification	Device	Drive Type	Capacity	Free	Type	Last Update
Datastorage7200r...	IBM Serial Attach...	Non-SSD	2,00 TB	813,71 GB	VMFS5	05/12/2017 19:32:43
datastore1	LSI Serial Attach...	Non-SSD	271,00 GB	270,05 GB	VMFS5	05/12/2017 19:32:43

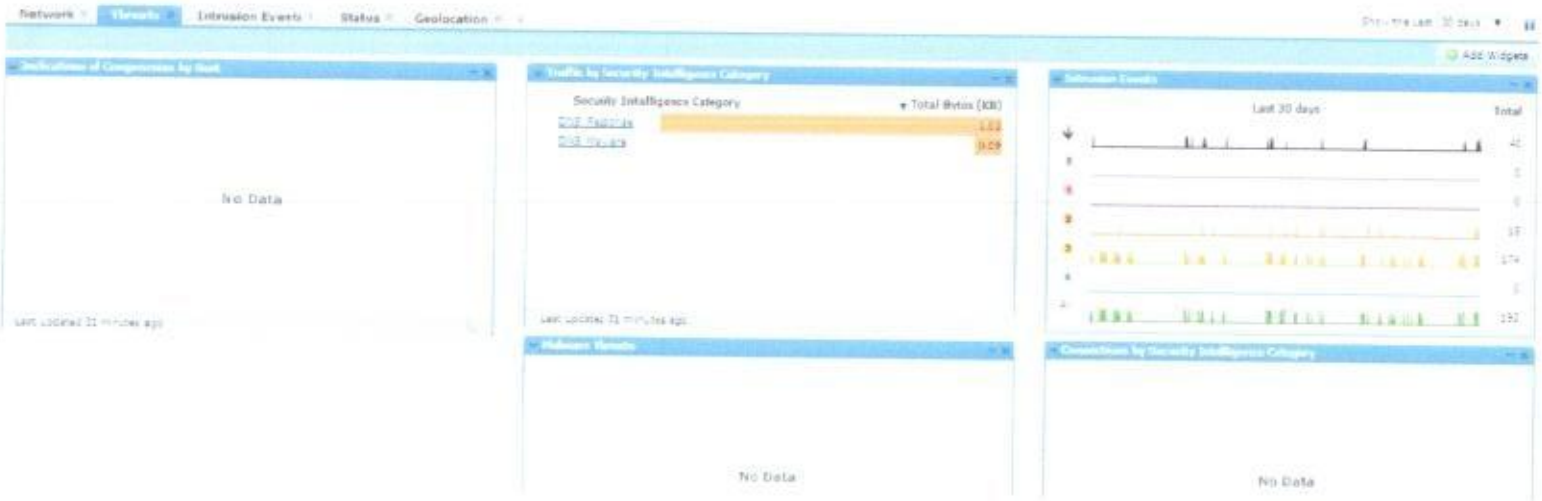
Estado del sistema Firewall

Data & Service

Revisar los siguientes equipos, se ha detectado eventos de seguridad

Tareas de backup a cintas

A nivel de eventos de DNS no se ha detectado en el último mes eventos



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

Data & Service

A nivel de DNS se han bloqueado ataques a nivel del Dominio

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category
	2017-12-04 07:54:50		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-29 11:34:14		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-29 09:50:31		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-28 09:21:30		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-28 07:07:50		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-27 17:43:06		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-24 07:30:11		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-23 10:29:47		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-23 10:10:44		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-23 09:39:21		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-23 08:46:40		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-22 14:30:46		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-22 14:15:41		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-21 10:14:22		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-20 07:13:05		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-14 08:09:07		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-14 08:03:11		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response
	2017-11-14 08:03:11		Domain Not Found	DNS Block	192.168.1.8		8.8.4.4	USA	DNS Response

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category
	[illegible]		Domain Not Found	DNS Block	192.168.1.1		No Authentication Required	8.8.8.8	USA	DNS Response

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

Top de sistemas operativos en la red

Trayectoria en la red de archivo con malware:

Events

Time	Event Type	Sending IP	Receiving IP	User	File Name	Dispo...	Action	Protocol	Client	Web Ap...	Description
2017-10-12 12:08:45	Transfer	52.67.183.127	192.168.1.138	No Authentication Re	TQ4PI9SReuIM82fc...	Unkno	Cloud Lookup Ti	HTTP	Chrome		Retrospective B
2017-10-13 04:57:59	Retrospectiv					Malware					
2017-10-26 02:20:16	Retrospectiv					Malware					

Data & Service

APLICACIONES CON ALTO RIESGO Y BAJA RELACIÓN CON EL NEGOCIO

Algunas aplicaciones conlleva n 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)
MyWay	446	Very High	Very Low	2.62
Zippyshare	53	Very High	Very Low	454.55
BitTorrent	53	Very High	Very Low	2.21
OnClick	3	Very High	Very Low	0.06
PornHub	0	Very High	Very Low	0.00

APLICACIONES CON CONSUMO ALTO DE ANCHO DE BANDA

Algunas aplicaciones usan una cantidad sustancial de ancho de banda de red. Este uso de ancho de banda puede ser costoso para su organización y puede afectar negativamente el rendimiento general de la red. Es posible que desee restringir el uso de estas aplicaciones a redes particulares: por ejemplo, una red inalámbrica puede no ser adecuada para la transmisión de video. O bien, puede cerrar completamente estas aplicaciones o simplemente obtener visibilidad de cómo se usa su ancho de banda.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MB)
Microsoft Update	36,592	Medium	Low	99,327.30
MPEG	1,917	Low	Medium	6,132.03
Flash Video	1,783	Low	Low	1,655.15
generic audio/video	190	Very Low	Medium	1,414.21
MP4	338	Very Low	Medium	1,214.75

Data & Service

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, 32.0.1700.102, 33.0.1750.170	5
Safari		0
Firefox	28.0, 40.0	4

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	20,085	143,175	116,065.84	92,103.68
Spyware and Adware	146	42,599	7,627.95	21,818.31
Peer to Peer	127	0	1,935.46	168.95
Malware Sites	46	7,035	28,668.67	5,772.45
Phishing and Other Frauds	33	1,026	281.10	946.06
Adult and Pornography	22	657	96,835.15	1,254.77
Cheating	4	0	50.03	6.09
Hacking	0	29	130.36	20.42
Proxy Avoid and Anonymizers	0	36	7.17	20.71

Data & Service

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.

OS VENDOR	OS VERSION	COUNT
Apple	7.1.1	1
CentOS	6.3, 6.4, 7.2, 7.3	1
Google	2.2.1, 2.2.2, 2.3 rev1, 2.3.1, 2.3.2, 2.3.3, 2.3.4, 2.3.5, 3.2.1, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.1, 4.2, 4.3, 4.4, 5.x, 7.0	1
Google	3701.81.2	1
Ubuntu	4.10 ppc, 10.04, 11.04, 12.10, 13.x, 14.04, 16.x	1

LOS ARCHIVOS QUE TRASLADAN SU RED

Downloads

FILE CATEGORY	FILE TYPE	PROTOCOL	COUNT
Archive	MSCAB	HTTP	35.200
PDF files	PDF	HTTP	768
Executables	MSEXE	HTTP	525
Archive	ZIP	HTTP	499
Archive	GZ	HTTP	299

Uploads

FILE CATEGORY	FILE TYPE	PROTOCOL	COUNT
PDF files	PDF	HTTP	136
Office Documents	WRI	HTTP	4
Office Documents	MAIL	HTTP	3
Office Documents	MDI	HTTP	2
Archive	ARJ	HTTP	1

Misc

FILE CATEGORY	FILE TYPE	PROTOCOL	COUNT
Office Documents	NEW_OFFICE	FTP Data	1,050
Executables	MSOLE2	FTP Data	874
PDF files	PDF	FTP Data	714
Executables	MSEXE	NetBIOS-ssn (SMB)	394
Office Documents	KLW	FTP Data	17

Revisar los siguientes equipos que se han detectado con eventos de seguridad bajos:

Lower Impact Events

ATTACKERS	ATTACKS
192.168.1.110	49
192.168.1.114	21
192.168.1.204	16
192.168.1.116	15
192.168.111.23	13