UNIVERSIDAD PEDAGÓGICA NACIONAL

INFORME DE EVALUACIÓN
DE LAS PROPUESTAS

CONVOCATORIA PÚBLICA

N°5 DE 2021

"CONTRATAR LA ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UNA NUEVA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL (CLÚSTER DE FIREWALLS) Y DE APLICACIONES (FIREWALLS DE APLICACIONES WEB) PARA LA UNIVERSIDAD PEDAGÓGICA NACIONAL"

BOGOTÁ D.C., DICIEMBRE DE 2021

UNIVERSIDAD PEDAGOGICA NACIONAL

Educadora de educadores

EVALUACIÓN JURÍDICA

CONVOCATORIA PÚBLICA N°5 DE 2021

INFORME DE EVALUACIÓN DE LOS REQUISITOS JURIDICOS DEL PROCESO DE SELECCIÓN MEDIANTE CONVOCATORIA PUBLICA NO. 05 DE 2021

VERIFICACIÓN DE REQUISITOS Y DOCUMENTOS DE CONTENIDO JURÍDICO

Se procede a la verificación de la capacidad jurídica de que trata el numeral 4.1 REQUISITOS JURÍDICOS HABILITANTES, de los Términos de Referencia, así:

.

PROPONENTE	SOFTSECURITY S.A.S. identificada con el NIT No. 900.031.953-1.			
REQUISITOS JURÍDICOS HABILITANTES	CUMPLE		FOLIOS	OBSERVACIONES
	SI	NO		
Fecha y hora de la presentación de la oferta	X			09/12/2021 1:58 P.M
1. CARTA DE PRESENTACIÓN DE LA OFERTA.	X		CD	Se presenta debidamente firmada por el Señor WILLIAM GUERRERO ALDANA, identificado con la cédula de ciudadanía No. 79.310.249, quien funge como representante legal suplente de la sociedad.
2. PODER	N/A	**N/A**	N/A	N/A
3. Autorización para Presentar Propuesta y Suscribir el Contrato	X	**N/A**	SUBSANACIÓN	Se efectuó requerimiento con el fin de que el proponente subsanara su propuesta toda ve que el representante legal tenia facultades limitadas en razón a la cuantía, de suerte que para el presente proceso requiere autorización previa del órgano competente. Así las cosas, durante el traslado procedió a entregar el documento que acredita que se encuentra facultado para participar en el proceso.
4. CERTIFICADO DE EXISTENCIA Y REPRESENTACIÓN LEGAL	X		CD	Se presenta certificado de existencia y representación legal de la Cámara de Comercio de Bogotá, de la sociedad SOFTSECURITY S.A.S. identificada con el NIT No. 900.031.953-1, expedido el 02/12/2021; cumpliendo con todo lo requerido.
5. CÉDULA DE CIUDADANÍA O DE EXTRANJERÍA DEL REPRESENTANTE LEGAL	X		5	La sociedad presenta Cédula de Ciudadanía de la representante Legal suplente, el Señor WILLIAM GUERRERO ALDANA, identificado con la cédula de ciudadanía No. 79.310.249.

INFORME DE EVALUACIÓN DE LOS REQUISITOS JURIDICOS DEL PROCESO DE SELECCIÓN MEDIANTE CONVOCATORIA PUBLICA NO. 05 DE 2021

PROPONENTE	SOFTSECURITY S.A.S. identificada con el NIT No. 900.031.953-1.			
REQUISITOS JURÍDICOS HABILITANTES	CUMPLE		FOLIOS	OBSERVACIONES
	SI	NO		
6. Documento de Conformación de Proponente Plural	N/A	**N/A**	N/A	N/A
7. CERTIFICACIÓN DE PAGO DE APORTES AL SISTEMA INTEGRAL DE SEGURIDAD SOCIAL Y PARAFISCALES	X		CD	Se presento certificado debidamente suscrito por el señor GUIOVANNA PARRADO DONOSO, identificado con la cédula de ciudadanía No. 52.229.358 Y T.P. No. 133149-T, quien funge como revisor fiscal de la sociedad.
8. DOCUMENTOS ADICIONALES	X			La Entidad verificó lo pertinente: • Al BOLETÍN DE RESPONSABLES FISCALES de la Contraloría General de la república; • Al CERTIFICADO DE ANTECEDENTES DISCIPLINARIOS de la Procuraduría General de la Nación; • Al CERTIFICADO SOBRE ANTECEDENTES PENALES de la Policía Nacional; • Al "Sistema Registro Nacional de Medidas Correctivas RNMC" (CONSULTA PAGO DE MULTAS – CODIGO DE POLICIA (Art. 183. Ley 1801 del 29 de julio de 2016 "Por la cual se expide el Código Nacional de Policía y Convivencia" – rige a partir del 29 de enero de 2017).
9. Registro Único Tributario – RUT	X		CD	Se presenta RUT de la sociedad SOFTSECURITY S.A.S. identificada con el NIT No. 900.031.953-1

INFORME DE EVALUACIÓN DE LOS REQUISITOS JURIDICOS DEL PROCESO DE SELECCIÓN MEDIANTE CONVOCATORIA PUBLICA NO. 05 DE 2021

PROPONENTE	SOFTSECURITY S.A.S. identificada con el NIT No. 900.031.953-1.			
REQUISITOS JURÍDICOS HABILITANTES	CUMPLE		FOLIOS	OBSERVACIONES
	SI	NO		
10. REGISTRO UNICO DE PROPONENTES	X		CD	Se presenta certificado de Registro Único de Proponentes expedido por la Cámara de Comercio de Bogotá, de la sociedad SOFTSECURITY S.A.S. identificada con el NIT No. 900.031.953-1, expedido el 07/12/2021, cumpliendo con todo lo requerido.
11. GARANTIA DE SERIEDAD DE LA OFERTA Y RECIBO DE PAGO	X		CD	El proponente aporta póliza 21-45-101353539 expedida por SEGUROS DEL ESTADO S.A., cumpliendo con el valor asegurado y la vigencia del amparo de seriedad de la oferta, y demás condiciones señaladas en el documento de términos de referencia.
CONCLUSIÓN	CUMPLE			

No siendo otro el objeto, se concluye el Informe de Evaluación Jurídica de los requisitos habilitantes Jurídicos del PROCESO DE SELECCIÓN MEDIANTE CONVOCATORIA PUBICA NO. 05 DE 2021.

NICOLAS ANDRES GUZMAN PADILLA
Evaluador Jurídico

EVALUACIÓN FINANCIERA

CONVOCATORIA PÚBLICA N°5 DE 2021

UNIVERSIDAD PEDAGOGICA NACIONAL
VICERRECTORIA ADMINISTRATIVA Y FINANCIERA
EVALUACION A LA CAPACIDAD FINANCIERA CONVOCATORIA PÚBLICA No. 005 DE 2021

Fecha **13/12/2021**

PRESUPUESTO OFICIAL: **1.188.166.991**

DOCUMENTOS (FOLIOS)

	PROPONENTE 1
	SOFTSECURITY S.A.S.
REGISTRO UNICO TRIBUTARIO -RUT-	150 - 154
REGISTRO UNICO DE PROPONENTES	155 - 215
(OTROS DOCUMENTOS QUE SEAN SOLICITADOS)	N/A

INFORMACION FINANCIERA

		INFORMACION DEL RUP			
	PROPONENTE	ACTIVO CORRIENTE	PASIVO CORRIENTE	ACTIVO TOTAL	PASIVO TOTAL
1	SOFTSECURITY S.A.S.	$ 4.690.481.049	$ 2.506.855.889	$ 6.103.664.176	$ 3.132.238.259

		RESULTADO DE EVALUACION FINANCIERA			
	PROPONENTE	INDICE DE LIQUIDEZ (= > 1,24 VECES)	NIVEL DE ENDEUDAMIENTO (=< AL 70%)	CAPITAL DE TRABAJO (> AL 40%)	VALOR PROPUESTA CON IVA
1	SOFTSECURITY S.A.S.	1,87	51,32%	$ 2.183.625.160	$ 1.185.999.934

RESULTADOS HABILITACION

	SOFTSECURITY S.A.S.
INDICE DE LIQUIDEZ (= > 1,24 VECES)	Si cumple
NIVEL DE ENDEUDAMIENTO (=< AL 70%)	Si cumple
CAPITAL DE TRABAJO (> AL 40%)	Si cumple
RESULTADO DE HABILITACIÓN	**HABILITADO**

Observaciones

De acuerdo al RUP presentado por el oferente, se tomó en cuenta la información financiera de 2020 conforme a lo establecido en el Decreto 579 de 2021.

Nota

El análisis realizado por esta Subdirección se limita a evaluar la capacidad financiera de los proponentes de acuerdo a los indicadores financieros y a determinar la habilitación de los mismos. Es importante destacar que los datos que se tomaron para dicha evaluación corresponden a lo establecido en el Decreto 579 de 2021. La oferta económica y sus componentes son revisadas y evaluadas por el área técnica que sea responsable del proceso.

JAIRO ALBERTO SERRATO ROMERO
Subdirector Financiero

Elaboró: Anderson Mora López - Profesional Universitario - Contabilidad
Revisó: Marysol Guerra Leguizamón - Profesional Especializado - Contabilidad

UNIVERSIDAD PEDAGOGICA NACIONAL

Educadora de educadores

EVALUACIÓN TÉCNICA

CONVOCATORIA PÚBLICA N°5 DE 2021

VICERRECTORIA ADMINISTRATIVA Y FINANCIERA

SUBDIRECIÓN DE GESTION DE SISTEMAS DE INFORMACIÓN

ACTA DE EVALUACIÓN TÉCNICA

CONVOCATORIA PÚBLICA No. 05 DE 2021

OBJETO: *"CONTRATAR LA ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UNA NUEVA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL (CLÚSTER DE FIREWALLS) Y DE APLICACIONES (FIREWALLS DE APLICACIONES WEB) PARA LA UNIVERSIDAD PEDAGÓGICA NACIONAL"*.

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

DESARROLLO DE LA EVALUACIÓN

Al proceso de CONVOCATORIA PÚBLICA No. 05 DE 2021, se presentó una (1) empresa, a saber:

- **SOFTSECURITY S.A.S**
  NIT: 900.031.953-1

1. CALIFICACIÓN DE LAS OFERTAS

ASPECTOS A EVALUAR:

FACTORES: FACTOR ECONÓMICO – VALOR DE LA PROPUESTA, FACTOR TECNICO – VALORES AGREGADOS

LA UNIVERSIDAD debe evaluar únicamente las Ofertas de los Proponentes que hayan acreditado los requisitos habilitantes solicitados.

La Universidad asignará el siguiente puntaje:

ITEM	CRITERIO DE EVALUACIÓN	MÁXIMO PUNTAJE
1	FACTOR ECONÓMICO – VALOR DE LA PROPUESTA	400
2	FACTOR TECNICO – VALORES AGREGADOS	600
	TOTAL	1000

a) FACTOR ECONÓMICO – VALOR DE PROPUESTA

Los términos de referencia de la CONVOCATORIA PUBLICA No. 5 DE 2021 dicen lo siguiente:

"La Universidad otorgará el máximo puntaje por este concepto (hasta 400 puntos), a la propuesta que, cumpliendo con la totalidad de requisitos habilitantes exigidos, ofrezca el menor precio total.

Sobre esta base se calificarán a las demás ofertas en forma proporcional, aplicando regla de tres inversas. Solo para este ítem".

Puntaje asignado: Teniendo en cuenta los valores presentados por el proponente y por ser el único que se presentó a la convocatoria pública, el puntaje asignado para este factor es de Cuatrocientos (400) puntos.

PROPONENTES	EVALUACION ECONOMICA Y FACTORES PONDERABLES DE LAS PROPUESTAS HABILITADAS

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	VR. PROPUESTA ANTES DE I.V.A	I.V.A	VR. TOTAL PROPUESTA	DIFERENCIA CONTRA PRESUPUESTO	PUNTAJE FACTOR ECONOMICO (Regla de Tres Inversa)
SOFTSECURITY S.A.S	$ 996.638.600	$ 189.361.334	**$ 1.185.999.934**	$ 2.167.057	400
PRESUPUESTO	**$ 1.188.166.991**				

b) FACTOR TÉCNICO – VALORES AGREGADOS

Los términos de referencia de la CONVOCATORIA PUBLICA No. 5 DE 2021 dicen lo siguiente:

"La Universidad otorgará el máximo puntaje por este concepto (hasta 600 puntos), a la propuesta que, cumpliendo con la totalidad de requisitos exigidos, ofrezca mayor valor agregado en el suministro de los Bienes con los estándares de calidad reconocidos en el sector".

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

PUNTAJES ASIGNADOS A LOS VALORES AGREGADOS (Proforma No. 6)

ITEM	CRITERIOS DE EVALUACIÓN PARA VALORES AGREGADOS	PUNTOS ASIGNADOS
1	Ofrecer una solución de administración de los firewalls por aparte con un appliance dedicado. Por mejores prácticas de implementación es siempre mejor tener la capa de protección separada de la capa de administración lo cual mejorara notablemente el rendimiento y performance de las comunicaciones, y segundo permitirá la continuidad de negocio, es decir, en caso de que la consola de administración falle, no se interrumpen las comunicaciones; si falla la consola de administración los firewalls siguen trabajando normalmente.	200
2	Ofrecer una solución de SOC, donde se realice un monitoreo	150
	en tiempo real de los equipos implementados durante la duración del contrato, para de esta manera ser lo más proactivo posibles ante cualquier fallo y/o error que se pueda presentar en la infraestructura ofertada	
3	Dar curso para dos (2) personas de certificación de la solución dictado directamente por el fabricante o por una entidad autorizada por el fabricante. Se debe entregar voucher para la presentación del examen de certificación y Carta del fabricante de la solución ofrecida en donde relacione las entidades autorizadas para dictar los cursos de certificación.	150
4	Dar curso de la solución para cinco (5) personas de la entidad dictado fuera de las instalaciones de la universidad por un ente certificado por el fabricante con entrega de certificado de asistencia	50
5	Transferencia de conocimiento y sensibilización de la norma ISO27000 y ISO27001 a los funcionarios de la unidad de sistemas de la UPN realizado en las instalaciones de la universidad (Aproximadamente 20 personas)	50
NOTA	Si no ofrece valor agregado el puntaje será de Cero (0) en el ítem correspondiente	0
	TOTAL	**600**

En la evaluación se tendrán en cuenta los aspectos anteriormente definidos y se asignarán los puntajes respectivos según ofrecimiento.

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

Puntaje asignado: Teniendo en cuenta que el proponente **OFRECIÓ** todos los valores agregados relacionados en la Proforma No. 6, el puntaje asignado para este factor es de seiscientos (600) puntos.

ITEM	VALORES AGREGADOS	OFRECE (SI/NO)	PUNTAJE ASIGNADO
1	Ofrecer una solución de administración de los firewalls por aparte con un appliance dedicado. Por mejores prácticas de implementación es siempre mejor tener la capa de protección separada de la capa de administración lo cual mejorara notablemente el rendimiento y performance de las comunicaciones, y segundo permitirá la continuidad de negocio, es decir, en caso de que la consola de administración falle, no se interrumpen las comunicaciones; si falla la consola de administración los firewalls siguen trabajando normalmente.	**SI**	**200**
2	Ofrecer una solución de SOC, donde se realice un monitoreo en tiempo real de los equipos implementados durante la duración del contrato, para de esta manera ser lo más proactivo posibles ante cualquier fallo y/o error que se pueda presentar en la infraestructura ofertada	**SI**	**150**
3	Dar curso para dos (2) personas de certificación de la solución dictado directamente por el fabricante o por una entidad autorizada por el fabricante. Se debe entregar voucher para la presentación del examen de certificación y Carta del fabricante de la solución ofrecida en donde relacione las entidades autorizadas para dictar los cursos de certificación	**SI**	**150**
4	Dar curso de la solución para cinco (5) personas de la entidad dictada fuera de la instalación de la universidad por un ente certificado por el fabricante con entrega de certificado de asistencia	**SI**	**50**
5	Transferencia de conocimiento y sensibilización de la norma ISO27000 y ISO27001 a los funcionarios de la unidad de sistemas de la UPN realizado en las instalaciones de la universidad (Aproximadamente 20 personas)	**SI**	**50**
		PUNTAJE TOTAL	**600**

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

EMPRESA	VALORES AGREGADOS	PUNTAJE	SE VERIFICA EN FOLIOS DESDE - HASTA
SOFTSECURITY S.A.S	CUMPLE	600	410 – 410

2. VERIFICACIÓN DE CUMPLIMIENTO DE REQUISITOS DE LAS OFERTAS

ASPECTOS A VERIFICAR:

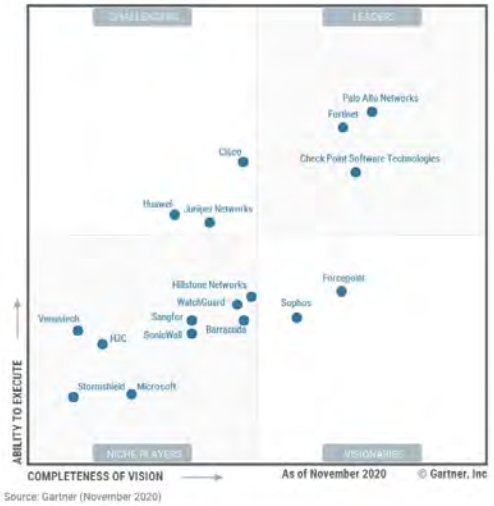
a) **REFERENTES Y CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS - (PROFORMA No. 4 - Especificaciones Técnicas).**
b) **VERIFICACIÓN DE LA EXPERIENCIA DEL PROPONENTE**
c) **CÓDIGOS RUP - REGISTRO ÚNICO DE PROPONENTES**

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

a) REQUERIMIENTOS EN EL NUMERAL 3.2. REFERENTES Y CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS - (PROFORMA No. 4 - Especificaciones Técnicas).

ÍTEM	REQUERIMIENTOS FIREWALL	Cumple (SI)	¿Cómo se verifica?	Revisión
A	**1. Requisitos generales**			
1	La UNIVERSIDAD PEDAGÓGICA NACIONAL desea una solución de seguridad perimetral para alrededor de 15.000 usuarios y 120 servidores, que tenga las capacidades de una solución de Prevención de Amenazas, el cual incluya los componentes de Firewall, Control de Aplicaciones, Control de Navegación, IPS, Control de Malware Conocido, Control de Malware Avanzado, VPN IPSec /SSL, Manejo de Identidades. La solución Ofertada debe proporcionarnos en Alta disponibilidad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Entregaremos a la UNIVERSIDAD PEDAGÓGICA NACIONAL una solución de seguridad perimetral para alrededor de 15.000 usuarios y 120 servidores, la cual tendrá las capacidades de una solución de Prevención de Amenazas, que incluye los componentes de Firewall, Control de Aplicaciones, Control de Navegación, IPS, Control de Malware Conocido, Control de Malware Avanzado, VPN IPSec /SSL, Manejo de Identidades. La solución que será entregada será proporcionada en Alta disponibilidad.	Verificado
2	Esta solución debe estar reconocida por Gartner como una solución líder en su cuadrante en los últimos 3 años	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución Checkpoint NGFW es reconocida por Gartner como una solución líder en su cuadrante en los últimos 3 años. **AÑO 2021**	

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			Magic Quadrant Figure 1: Magic Quadrant for Network Firewalls  **AÑO 2020** Magic Quadrant Figure 1. Magic Quadrant for Network Firewalls  Source: Gartner (November 2020)	Verificado

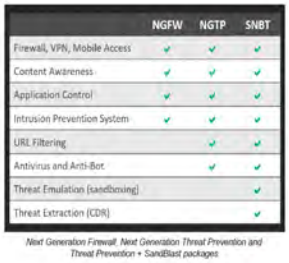
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			AÑO 2019 	
3	Los registros (logs) de la solución de seguridad perimetral descritas, deben centralizarse en una única consola central de gestión, que permita generar reportes y correlacionar eventos según el impacto de seguridad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Los registros (logs) de la solución de seguridad perimetral descritas, se centralizan en una única consola central de gestión, la cual permite generar reportes y correlacionar eventos según el impacto de seguridad. Ver **smartevent-datasheet.pdf paginas 1,2,3,4**	Verificado
4	La entidad requiere, que las capas de Plano de Control (Gestión) y Plano de Datos (Componentes de Protección) estén completamente separados tal como lo sugiere el modelo Zero Trust	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución ofrecida está basada en el modelo de Zero Trust, incluimos dentro de la arquitectura de la solución un appliance de administración independiente **SMART-1** (Plano de Control (Gestión)) (ver **smart-1-security-management-platform-datasheet.pdf modelo Smart-1 600S**) y dos gateway **(ver 7000-security-gateway-datasheet.pdf modelo 7000 CPAP-SG7000-PLUS-SNBT)** separados de la administración y configurados en alta disponibilidad (Componentes de Protección) como lo sugiere el modelo Zero Trust.	Verificado

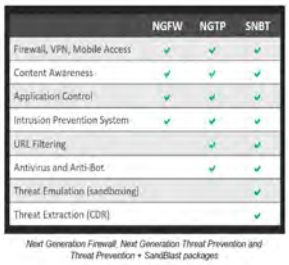
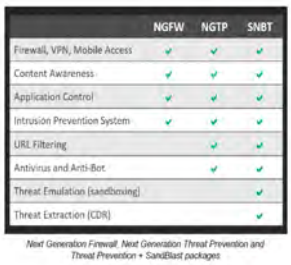
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	(http://go.forrester.com)			
5	Los gateway deben estar en alta disponibilidad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución ofrecida se compone de dos gateway **(7000-security-gateway-datasheet.pdf modelo 7000 CPAP-SG7000-PLUS-SNBT),** los cuales serán implementados en alta disponibilidad. Ver CP_R81_ClusterXL_AdminGuide.pdf pagina 35. Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf páginas 340**	Verificado
6	La solución debe incluir el licenciamiento full de NGFW	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución ofrecida incluye el licenciamiento full de NGFW. Ver **7000-security-gateway-datasheet.pdf** página 2 - CPAP-SG7000-PLUS-SNBT.	Verificado
7	La solución debe incluir el licenciamiento o uso de vpn tipo IPSec y SSL para usuarios ilimitados	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución ofrecida incluye el licenciamiento llamado **Mobile Access Blade unlimited (CPSB-MOB-U)** el cual permite el uso de vpn tipo IPSec y SSL para usuarios ilimitados. Ver **mobile-access-datasheet.pdf**	Verificado
8	El año de lanzamiento de los Appliances Gateway debe ser mínimo 2020 en adelante.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Los Appliances Gateway son el modelo 7000 de Checkpoint y fueron lazados por el fabricante en el año 2020.Ver https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk139932 	Verificado
9	El soporte, licenciamiento y garantía del fabricante ofertado deberá ser por 1 año y debe incluir soporte de fábrica 7x24 y del proveedor 7x24.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Con la solución ofrecida entregaremos el licenciamiento y garantía del fabricante por 1 año. Softsecurity en un Partner de Checkpoint con el status de “Certified Support Provider CCSP” lo cual nos permite recibir soporte directo por parte del fabricante 7x24 para la Universidad Pedagogica Nacional, es decir que la UPN contará con soporte de fabrica 7x24 y por parte del proveedor 7x24.	Verificado
10	El Gateway de próxima generación debe ser capaz de soportar estas aplicaciones de	**ENTERADOS, ACEPTAMOS Y**	Los Gateway Checkpoint firewall de próxima generación (next generation firewall) son capaces de soportar estas aplicaciones de seguridad de próxima generación en una plataforma unificada.	Verificado

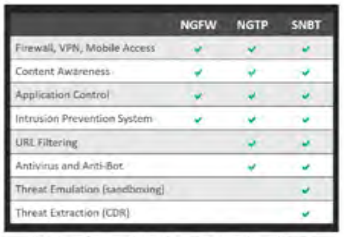
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	seguridad de próxima generación en una plataforma unificada.	**CUMPLI MOS**		
11	Stateful Inspection Firewall	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver **stateful-inspection-technology.pdf**	Verificado
12	Sistema de Prevención de Intrusión	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver **7000-security-gateway-datasheet.pdf página 2 (Intrusion Prevention System)**  Next Generation Firewall, Next Generation Threat Prevention and Threat Prevention + SandBlast packages **All-inclusive Security Solutions** Check Point 7000 security gateways include all security technologies including the SandBlast (sandboxing) software package for one year. Purchase a renewal for NGFW, NGTP or SandBlast (SNBT) for subsequent years as you like. Ver **CP_R81_NextGenSecurityGateway_Guide.pdf página 43** Ver **CP_R81_ThreatPrevention_AdminGuide.pdf**	Verificado
13	Adquisición de identidad de usuarios	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver **check-point-identity-awareness-datasheet.pdf** Ver **CP_R81_NextGenSecurityGateway_Guide.pdf página 43**	Verificado
14	Control de aplicaciones y filtrado de URL	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver **7000-security-gateway-datasheet.pdf página 2 (Application control – URL filtering)**	

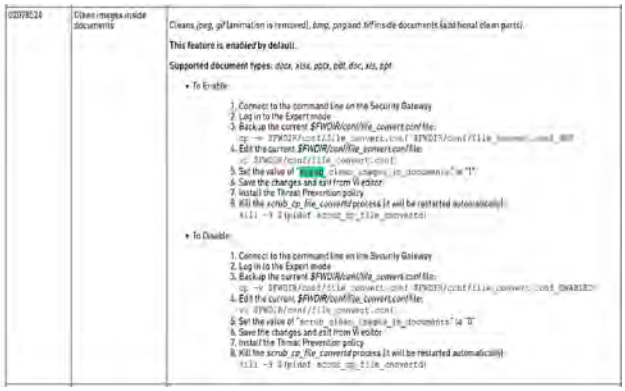
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			 **All-inclusive Security Solutions** Check Point 7000 security gateways include all security technologies including the SandBlast (sandboxing) software package for one year. Purchase a renewal for NGFW, NGTP or SandBlast (SNBT) for subsequent years as you like. https://www.checkpoint.com/quantum/url-filtering/ https://www.checkpoint.com/quantum/application-control/ Ver **CP_R81_NextGenSecurityGateway_Guide.pdf página 46 y 47**	Verificado
15	Control de Bots & Botnets, actualización periódica desde servicio en la nube propio	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **ds-anti-bot.pdf** Ver **7000-security-gateway-datasheet.pdf página 2 (Application control – URL filtering)**  **All-inclusive Security Solutions** Check Point 7000 security gateways include all security technologies including the SandBlast (sandboxing) software package for one year. Purchase a renewal for NGFW, NGTP or SandBlast (SNBT) for subsequent years as you like.	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			Ver “Threat Prevention” **CP_R81_NextGenSecurityGateway_Guide.pdf página 36** Ver **CP_R81_ThreatPrevention_AdminGuide.pdf**	
16	Anti - Virus	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **antivirus-datasheet.pdf** Ver **7000-security-gateway-datasheet.pdf página 2 (Application control – URL filtering)**  *Next Generation Firewall, Next Generation Threat Prevention and Threat Prevention + SandBlast packages* **All-inclusive Security Solution** Check Point 7000 security include all security tech including the SandBlast (san software package for one year. a renewal for NGFW, NGTP or S (SNBT) for subsequent years as Ver “Threat Prevention” **CP_R81_NextGenSecurityGateway_Guide.pdf página 36** Ver **CP_R81_ThreatPrevention_AdminGuide.pdf**	Verificado
17	Emulación de amenazas (Sandboxing)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf páginas 27, 33, 96, 97, 102**	Verificado

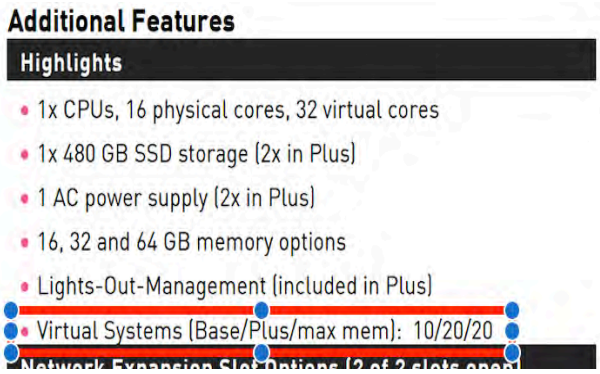
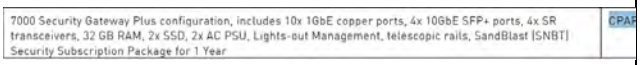
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

18	Extracción de amenazas (Depuración)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf páginas 27, 30, 31, 81, 82, 83**	Verificado
19	Data Scrubbing – Limpieza de Datos/Archivos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf (scrub) páginas 109, 110, 111,112, 194, 285, 286**  **https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk114613**	Verificado
20	Inspección de HTTPS	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf páginas 253**	Verificado
21	Reconocimiento de identidad de usuarios	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **check-point-identity-awareness-datasheet.pdf** Ver **CP_R81_NextGenSecurityGateway_Guide.pdf página 43**	Verificado

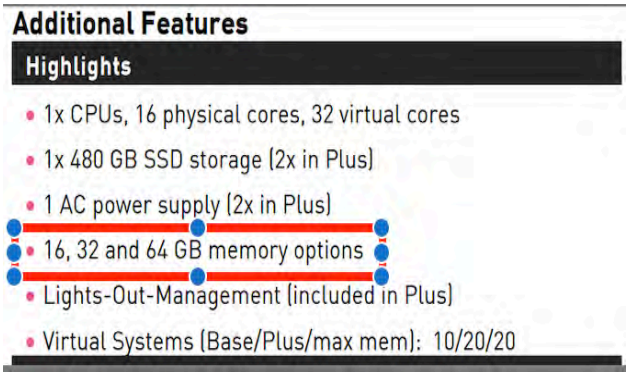
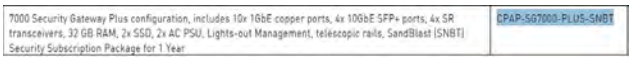
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

22	Anti - Spam	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf páginas 276, 277**	Verificado
23	VPN IPSec	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**CP_R81_RemoteAccessVPN_AdminGuide.pdf página 24** Ver **mobile-access-datasheet.pdf página 1**	Verificado
24	Acceso Seguro para dispositivos móviles Android y IOS mediante el uso de agentes para VPN, para usuarios ilimitados de la entidad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución ofrecida incluye el licenciamiento llamado **Mobile Access Blade unlimited (CPSB-MOB-U)** el cual permite el uso de vpn tipo IPSec y SSL para usuarios ilimitados. Ver **mobile-access-datasheet.pdf**	Verificado
25	Gestión de políticas de seguridad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf páginas 45, 173-177, 195,199,**	Verificado
26	Monitoreo y registro de logs	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf páginas 178** Ver **smartevent-datasheet.pdf**	Verificado
27	Almacenamiento de logs y estados de la plataforma	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81.10_LoggingAndMonitoring_AdminGuide.pdf páginas 25 – 28** **Ver CP_R81_Gaia_AdminGuide.pdf páginas 31**	Verificado
28	Correlación de logs, eventos, generación de acciones automáticas de respuesta ante incidentes e informe	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **smartevent-datasheet.pdf página 3 - 4**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

29	Virtualización de firewalls (sistemas virtuales)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 3**  Ver **virtual-systems-datasheet.pdf**	Verificado
30	Si requieren appliance adicionales para la administración de la solución o almacenamiento de logs para la solución estos deberán ser físicos propios del fabricante	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución propuesta incluye un appliance de administración y logs, dedicado propio del fabricante Checkpoint ver **smart-1-security-management-platform-datasheet.pdf modelo Smart-1 600S**)	Verificado
31	La plataforma debe incluir sistema operativo de 64 bits	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ReleaseNotes.pdf página 22**	Verificado
32	Los equipos Gateway debe soportar más de 32 GB de memoria RAM.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 3 - 4 - CPAP-SG7000-PLUS-SNBT** 	

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

				Verificado
33	Los equipos Gateway deben soportar como mínimo 8 interfaces 1G en cobre y/o fibra y 8 interfaces 10G en fibra, deben tener la posibilidad de realizar agregación entre las interfaces (LACP). Se deben incluir los diferentes SFP	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 3 - 4 - CPAP-SG7000-PLUS-SNBT, el equipo base incluye 10 interfases de 1G y un modulo de 4 interfases de 10G en fibra óptica SR, adicionalmente se incluirá un segundo módulo con 4 interfases de 10G en fibra óptica SR. Se incluirán los diferentes módulos SFP.**  Ver **CP_R81_Gaia_AdminGuide.pdf página 108 – (LACP)**	Verificado
34	Debe tener la opción de contar con una interfaz de administración (out-of-band) que permita las siguientes acciones sobre el equipo:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **LOM_Card_HTML5-based_6k_7k_16k_26k_28k_TE2000XN_AdminGuide.pdf página 32, 33, 35, 37, 38,39,40,41,42.** **SNMP ver CP_R81_Gaia_AdminGuide.pdf página 240**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	a. Encender la caja de manera remota			Verificado
	b. Acceso remoto a través de consola virtual KVM			Verificado
	c. Instalación remota utilizando una media virtual.			Verificado
	d. Para solución de problemas debe permitir el conocer el último estado de la caja antes de reiniciarse			Verificado
	e. Monitoreo de estado a través del protocolo SNMP			Verificado
35	Los componentes de la solución deben ser accesibles a través de SSH y de interfaz Web usando SSL.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ver CP_R81_Gaia_AdminGuide.pdf página 35 ssh y https página 56**	Verificado
36	La solución debe tener soporte IPv6 como mínimo para IPS, Control de Aplicaciones, Firewall, Modulo de Adquisición de Identidades, Filtrado URL, Antivirus and Control de Bots.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Gaia_AdminGuide.pdf pagina 23** Ver **https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk163313**	Verificado
37	Debe soportar la integración con Active Directory sin importar si es IPv4 o IPv6	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	El modulo que permite la integración con Active Directory se llama Identinty Awareness y este modulo está soportado para IPV4 o IPV6. Ver	Verificado

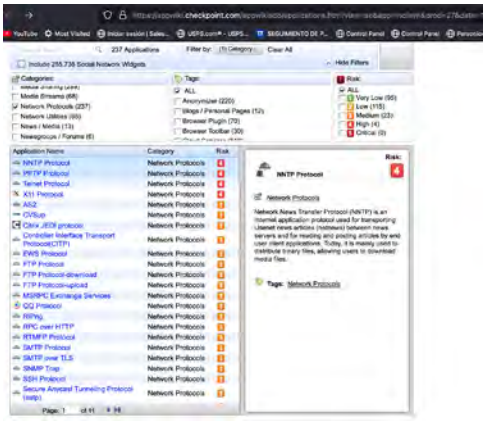
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk163313 • Several Software Blades in either Security Gateway mode or VSX mode (includes Firewall, Identity Awareness, Application Control, UR Protection), Anti-Bot, Anti-Virus, Anti-Malware, Threat Emulation, and Threat Extraction)	
38	La solución debe soportar de forma mínima y oficial, las siguientes características/RFC. Que permitirán un perfecto acoplamiento de la entidad con el decreto 2710 del Ministerio de Tecnologías de la Información y las comunicaciones, que habla de la implementación de IPv6 en el Gobierno de Colombia.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk163313 Supported IPv6 RFCs • RFC 1981 - Path Maximum Transmission Unit Discovery for IPv6 • RFC 2460 - IPv6 Basic specification • RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks • RFC 3596 - DNS Extensions to support IPv6 • RFC 4007 - IPv6 Scoped Address Architecture • RFC 4193 - Unique Local IPv6 Unicast Addresses • RFC 4213 - Basic Transition Mechanisms for IPv6 Hosts and Routers - 6in4 tunnel is support • RFC 4291 - IPv6 Addressing Architecture (which replaced RFC1884) • RFC 4443 - ICMPv6 • RFC 4861 - Neighbor Discovery • RFC 4862 - IPv6 Stateless Address Auto-configuration • RFC 2462 - IPv6 Stateless Address Auto-configuration • RFC 4007 - IPv6 Scoped Address Architecture • RFC 5952 - A Recommendation for IPv6 Address Text Representation	Verificado
	a. RFC 1981 - Path Máximum Transmission Unit Discovery for IPv6			Verificado
	b. RFC 2460 - IPv6 Basic specification			Verificado
	c. RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks			Verificado
	d. RFC 3596 - DNS Extensions to support IPv6			Verificado
	e. RFC 4007 - IPv6 Scoped Address Architecture			Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	f. RFC 4193 - Unique Local IPv6 Unicast Addresses			Verificado
	g. RFC 4213 - Basic Transition Mechanisms for IPv6 Hosts and Routers – 6in4 tunnel is supported.			Verificado
	h. RFC 4291 IPv6 Addressing Architecture (which replaced RFC1884)			Verificado
	i. RFC 4443 ICMPv6			Verificado
	j. RFC 4861 Neighbor Discovery			Verificado
39	La herramienta debe ser capaz de realizar backup/restores de la configuración, permitiendo al administrador programar la realización de los backups en el tiempo deseado.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Gaia_AdminGuide.pdf página 79**	Verificado
40	Los Backups pueden ser almacenados localmente y/o remotamente	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Gaia_AdminGuide.pdf página 79, 80, 81, 444,**	Verificado
41	**2. Requisitos para el Firewall de próxima generación**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Verificado
42	El Gateway de seguridad debe usar Stateful inspection basado en el análisis granular de la comunicación y el estado de las	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **stateful-inspection-technology.pdf**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	aplicaciones para rastrear y controlar el flujo de la red.			
43	La solución debe ser basada en Stateful Inspection, permitiendo crear reglas por puerto, protocolo y aplicación.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **stateful-inspection-technology.pdf página 3, 6**	Verificado
44	La solución debe admitir el control de acceso para al menos 150 servicios / protocolos / predefinidos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Checkpoint admite más de 230 servicios/protocolos predefinidos  https://appwiki.checkpoint.com/appwikisdb/applications.htm?view=se&app=inclient&prod=27&date=1&oem=737870118&dest=appwiki	Verificado
45	Debe proporcionar estadísticas de recuento de aciertos en las reglas de seguridad a la aplicación de administración de la plataforma.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 229,230,231**	Verificado
46	Debe permitir que las reglas de seguridad se apliquen en intervalos de tiempo	**ENTERADOS, ACEPTAMOS Y**	Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 157, 201.**	Verificado

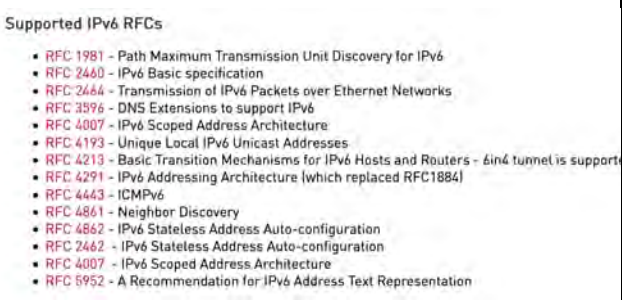
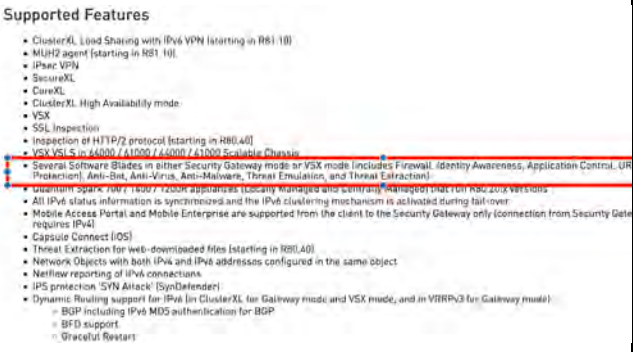
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	que se configurarán con una fecha / hora de caducidad. Debe tener la posibilidad de definir expiración de reglas de forma automática, por fecha & hora.	**CUMPLIMOS**	Ver **https://community.checkpoint.com/t5/Management/R80-10-Network-Access-Rule-expiration/td-p/21836**	
47	El firewall debe admitir los métodos de autenticación de usuario, cliente y sesión.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R76/CP_R76_SGW_WebAdmin/6721.htm **Authentication Methods** Instead of creating a security rule that simply allows or denies connections, the firewall administrator can request that clients authenticate when they try to access specific network resources. There are three authentication methods available: user, client and session. These methods differ in the services provided, the logon mechanism, and the overall user experience. Each method can be configured to connect and authenticate clients to the gateway before the connection is passed to the desired resource (a process known as nontransparent authentication). Alternatively, each method can be configured to connect clients directly to the target server (a process known as transparent authentication).	Verificado
48	Los siguientes esquemas de autenticación de usuario deben ser compatibles con el gateway de seguridad y el módulo VPN: tokens (ejemplo, SecureID), TACACS, RADIUS y certificados digitales	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R76/CP_R76_Mobile_Access_WebAdmin/41587.htm https://sc1.checkpoint.com/documents/R76/CP_R76_SGW_WebAdmin/6721.htm	Verificado
49	La solución debe incluir una base de datos de usuarios local, para permitir la autenticación y autorización de usuarios sin la necesidad de un dispositivo externo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_RemoteAccessVPN_AdminGuide.pdf página 51**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

50	La solución debe soportar protocolo DHCP, tanto servidor, como relay	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Gaia_AdminGuide.pdf páginas 175 – 183, 228, 235, 321**	Verificado
51	La solución debe soportar ser proxy de HTTP y HTTPS	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf páginas 184** Ver **CP_R81_NextGenSecurityGateway_Guide.pdf página 60**	Verificado
52	La solución debe incluir la capacidad de trabajar en modo Transparente / modo bridge	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	El modo transparente es el modo bridge. Ver **CP_R81_NextGenSecurityGateway_Guide.pdf página 170**	Verificado
53	La solución debe admitir alta disponibilidad de los dispositivos en modo activo pasivo y en modo compartición de carga. Ambos con sincronización de estados.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ClusterXL_AdminGuide.pdf paginas 46 y 47.**	Verificado
54	Soporte IPv6	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk163313**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

				
55	La solución debe soportar la configuración de doble stack (IPv4 e IPv6) en cualquier interfaz, sub interfaz o bond de las mismas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Gaia_AdminGuide.pdf página 276, 324, 86**	Verificado
56	La solución debe admitir el manejo del tráfico IPv6 como mínimo en los módulo IPS y APP, firewall, reconocimiento de identidad, filtrado de URL, antivirus y anti-Bot	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk163313** 	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

57	La solución debe admitir NAT 6 a 4 NAT o túneles 6 a 4.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf páginas 248-260.** Ver **CP_R81_NextGenSecurityGateway_Guide.pdf página 498**	Verificado
58	La solución debe ser compatible con la integración de AD usando el tráfico ipv6	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	El modulo que permite la integración con Active Directory se llama Identinty Awareness y este modulo está soportado para IPV4 o IPV6. Ver **https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk163313** • Several Software Blades in either Security Gateway mode or VSX mode [includes Firewall, Identity Awareness, Application Control, UR Protection], Anti-Bot, Anti-Virus, Anti-Malware, Threat Emulation, and Threat Extraction]	Verificado
59	La plataforma deberá admitir la capacidad de mostrar la tabla de enrutamiento IPv6	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Gaia_AdminGuide.pdf página 328**	Verificado
60	La solución debe soportar los siguientes RFC de IPv6:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk163313**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

61	RFC 1981 Path Máximum Transmission Unit Discovery for IPv6	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Supported IPv6 RFCs • RFC 1981 - Path Maximum Transmission Unit Discovery for IPv6 • RFC 2460 - IPv6 Basic specification • RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks • RFC 3596 - DNS Extensions to support IPv6 • RFC 4007 - IPv6 Scoped Address Architecture • RFC 4193 - Unique Local IPv6 Unicast Addresses • RFC 4213 - Basic Transition Mechanisms for IPv6 Hosts and Routers - 6in4 tunnel is support • RFC 4291 - IPv6 Addressing Architecture (which replaced RFC1884) • RFC 4443 - ICMPv6 • RFC 4861 - Neighbor Discovery • RFC 4862 - IPv6 Stateless Address Auto-configuration • RFC 2462 - IPv6 Stateless Address Auto-configuration • RFC 4007 - IPv6 Scoped Address Architecture • RFC 5952 - A Recommendation for IPv6 Address Text Representation	Verificado
62	RFC 2460 IPv6 Basic specification	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
63	RFC 2464 Transmission of IPv6 Packets over Ethernet Networks	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
64	RFC 3596 DNS Extensions to support IPv6	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
65	RFC 4007 IPv6 Scoped Address Architecture	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
66	RFC 4193 Unique Local IPv6 Unicast Addresses	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
67	RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers – 6in4 tunnel is supported.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
68	RFC 4291 IPv6 Addressing	**ENTERADOS, ACEPTAMOS Y**		Verificado

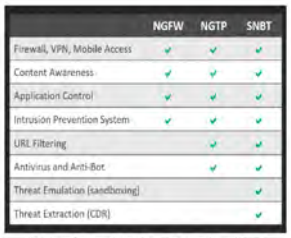
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	Architecture (which replaced RFC1884)	**CUMPLIMOS**		
69	RFC 4443 ICMPv6	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
70	RFC 4861 Neighbor Discovery	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
71	RFC 4862 IPv6 Stateless Address Auto-configuration	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
B	**Sistema de Prevención de Intrusión**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	
1	El proveedor debe proporcionar evidencia de la posición de liderazgo en los últimos 3 años del Cuadrante Mágico de Gartner para las soluciones de Prevención de Intrusión y / o el Cuadrante Mágico Gartner de firewall de red empresarial.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución Checkpoint NGFW es reconocida por Gartner como una solución líder en su cuadrante en los últimos 3 años. **AÑO 2021**	Verificado

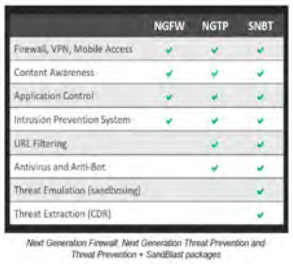
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			Magic Quadrant Figure 1: Magic Quadrant for Network Firewalls  **AÑO 2020**  Source: Gartner (November 2020)	

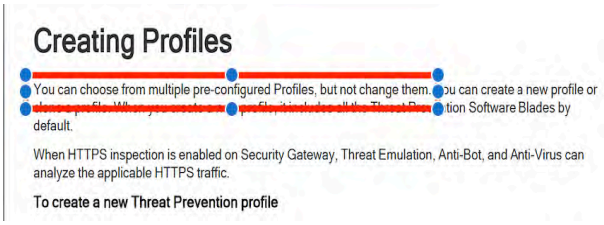
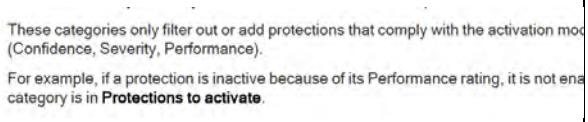
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			AÑO 2019  	
2	El módulo de Prevención de Intrusiones 'IPS' debe estar integrado en la plataforma de Firewall de nueva Generación.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 2 (Intrusion Prevention System)**  **All-inclusive Security Solutions** Check Point 7000 security gateways include all security technologies including the SandBlast (sandboxing) software package for one year. Purchase a renewal for NGFW, NGTP or SandBlast (SNBT) for subsequent years as you like. Ver **CP_R81_NextGenSecurityGateway_Guide.pdf página 43** Ver **CP_R81_ThreatPrevention_AdminGuide.pdf**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

3	El IPS debe basarse en los siguientes mecanismos de detección: firmas de explotación, anomalías de protocolo, controles de aplicaciones y detección basada en el comportamiento	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 27, 28, 29**	Verificado
4	IPS y el módulo de firewall deben integrarse en una plataforma.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	El modulo de IPS y el modulo de firewall están integrados en una única plataforma. Ver **7000-security-gateway-datasheet.pdf página 2 (Intrusion Prevention System)**  *Next Generation Firewall, Next Generation Threat Prevention and Threat Prevention + SandBlast packages* **All-inclusive Security Solutions** Check Point 7000 security gateways include all security technologies including the SandBlast (sandboxing) software package for one year. Purchase a renewal for NGFW, NGTP or SandBlast (SNBT) for subsequent years as you like. Ver **CP_R81_NextGenSecurityGateway_Guide.pdf página 43** Ver **CP_R81_ThreatPrevention_AdminGuide.pdf**	Verificado
5	El módulo de Prevención de Intrusiones 'IPS', debe ser capaz de tener una opción para proteger solo los activos internos, en caso de ser requerido.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver "Protected Scope", client and server protection **CP_R81_ThreatPrevention_AdminGuide.pdf página 50, 51, 66**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

6	IPS debe tener opciones para crear perfiles para las protecciones basadas en el cliente o servidor, o una combinación de ambos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver client and server protection **CP_R81_ThreatPrevention_AdminGuide.pdf página 66**	Verificado
7	IPS debe proporcionar al menos dos perfiles / políticas predefinidos que se puedan usar de inmediato	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver "Creating Profiles" **CP_R81_ThreatPrevention_AdminGuide.pdf página 57** 	Verificado
8	IPS debe tener un mecanismo de apertura de fallas basado en software, configurable basado en umbrales de CPU de puertas de enlace de seguridad y uso de memoria	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver "Creating Profiles" **CP_R81_ThreatPrevention_AdminGuide.pdf página 66, 210, 211** 	

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			To bypass IPS inspection under heavy load Step / Instructions 1 In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway. The gateway window opens and shows the **General Properties** page. 2 From the navigation tree, click IPS. 3 Select **Bypass IPS inspection when gateway is under heavy load**. 4 To set logs for activity while IPS is off, in the **Track** drop-down list, select a tracking method. 5 To configure the definition of heavy load, click **Advanced**. 6 In the **High** fields, provide the percentage of **CPU Usage** and **Memory Usage** that defines Heavy Load, at which point IPS inspection will be bypassed. 7 In the **Low** fields, provide the percentage of **CPU Usage** and **Memory Usage** that defines a return from Heavy Load to normal load.	Verificado
9	IPS debe proporcionar un mecanismo automatizado para activar o administrar nuevas firmas a partir de actualizaciones	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 65, 66, 67, 167-172, 173**	Verificado
10	IPS debe admitir excepciones de red basadas en la fuente, el destino, el servicio o una combinación de los tres	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 91, 92, 93, 94,**	Verificado
11	IPS debe incluir un modo de solución de problemas que establece el perfil en uso en modo de detección (sin bloquear trafico), con un click sin modificar las protecciones individuales	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **intrusion-prevention-system-ips-datasheet.pdf página 2**	Verificado
12	La aplicación IPS debe tener un mecanismo centralizado de	**ENTERADOS, ACEPTAMOS Y**	Los registros (logs) de la solución de seguridad perimetral descritas, se centralizan en una única consola central de gestión, la cual permite generar reportes y correlacionar eventos según el	Verificado

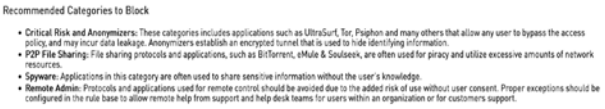
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	correlación e informe de eventos	**CUMPLIMOS**	impacto de seguridad. Ver **smartevent-datasheet.pdf paginas 1,2,3,4**	
13	El IPS debe proveer de un mecanismo automático, para activar o administrar nuevas firmas de protección, desde el proceso de actualización de este componente.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 171 – 174** Ver **intrusion-prevention-system-ips-datasheet.pdf página 1**	Verificado
14	El administrador debe poder activar automáticamente nuevas protecciones, en función de parámetros configurables (impacto en el rendimiento, gravedad de la amenaza, nivel de confianza, protecciones del cliente, protecciones del servidor)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 167-174, 66** Ver https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92707.htm “Browsing IPS Protections”	Verificado
15	IPS debe ser capaz de detectar y prevenir las siguientes amenazas: uso indebido de protocolos, comunicaciones de malware, intentos de tunelización y tipos de ataques genéricos sin firmas predefinidas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **intrusion-prevention-system-ips-datasheet.pdf página 1** Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 27, 28, 29**	Verificado
16	Para cada protección, la solución debe incluir el tipo de protección (relacionada con el servidor o con el cliente), la gravedad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 66,167** Ver **intrusion-prevention-system-ips-datasheet.pdf página 2**	Verificado

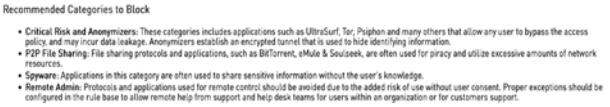
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	de la amenaza, el impacto en el rendimiento, el nivel de confianza y la referencia de la industria.			
17	El IPS deberá contar con una guía visual para el administrador, que le permita categorizar la severidad de las firmas, si la seguridad protege la comunicación del lado del cliente o del servidor al que se accede.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 167,168,66**	Verificado
18	IPS debe ser capaz de recopilar una captura de paquetes para protecciones específicas	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 186, 187**	Verificado
19	El IPS debe tener un mecanismo de Fail-Open basado en Software, que permita el funcionamiento del appliance en caso de consumos altos de CPU y/o Memoria RAM.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 210, 190**	Verificado
20	IPS debe poder detectar y bloquear los ataques a la red y a la capa de aplicaciones, protegiendo al menos los siguientes servicios: servicios de correo electrónico, DNS, FTP, servicios de Windows (redes de Microsoft)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 210** Ver **intrusion-prevention-system-ips-datasheet.pdf página 1** **Ver** https://sc1.checkpoint.com/documents/R77/CP_R77_IPS_WebAdminGuide/12857.htm#o12879	Verificado

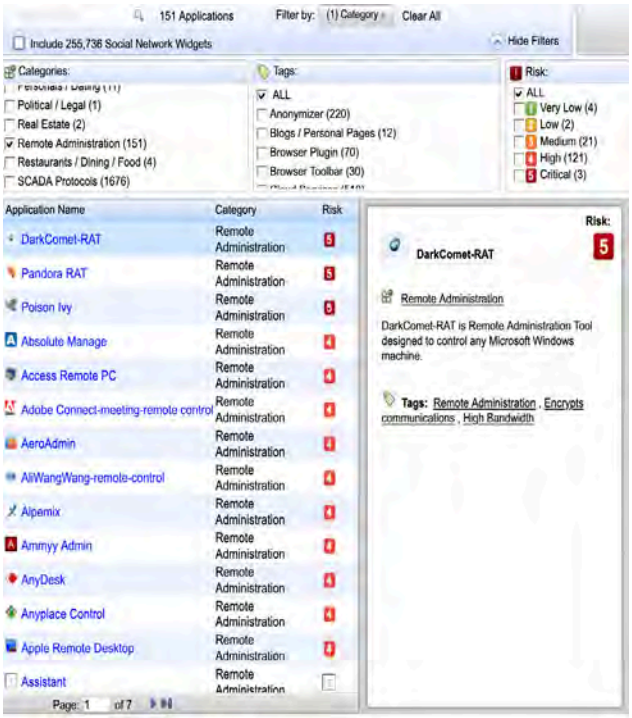
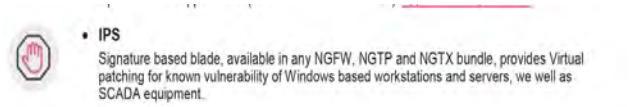
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

21	El proveedor debe proporcionar evidencia de liderazgo para proteger las vulnerabilidades de Microsoft	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://www.checkpoint.com/quantum/intrusion-prevention-system-ips/ 	Verificado
22	IPS y / o Application Control deben incluir la capacidad de detectar y bloquear aplicaciones P2P y evasivas	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk112249  Ver **intrusion-prevention-system-ips-datasheet.pdf página 1 “Evasive attack methods”**	Verificado
23	El administrador debe ser capaz de definir exclusiones de red y host de la inspección de IPS	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 91** Ver	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92707.htm "Adding Network Exceptions"	
24	La solución debe proteger contra el envenenamiento de caché de DNS e impide que los usuarios accedan a las direcciones de dominio bloqueadas	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk35624	Verificado
25	La solución debe proporcionar protecciones de protocolos VOIP	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R76/CP_R76_VoIP_WebAdmin/87691.htm Ver **CP_R81_VoIP_AdminGuide.pdf página 17**	Verificado
26	IPS y / o Application Control deben detectar y bloquear las aplicaciones de controles remotos, incluidas aquellas que son capaces de crear túneles a través del tráfico HTTP.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk112249  Recommended Categories to Block • **Critical Risk and Anonymizers:** These categories includes applications such as UltraSurf, Tor, Psiphon and many others that allow any user to bypass the access policy, and may incur data leakage. Anonymizers establish an encrypted tunnel that is used to hide identifying information. • **P2P File Sharing:** File sharing protocols and applications, such as BitTorrent, eMule & Soulseek, are often used for piracy and utilize excessive amounts of network resources. • **Spyware:** Applications in this category are often used to share sensitive information without the user's knowledge. • **Remote Admin:** Protocols and applications used for remote control should be avoided due to the added risk of use without user consent. Proper exceptions should be configured in the rule base to allow remote help from support and help desk teams for users within an organization or for customers support. Ver	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			https://sc1.checkpoint.com/documents/R76/CP_R76_AppControl_WebAdmin/60923.htm “Remote Access application” 	
27	IPS debe tener protecciones SCADA	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **critical-infrastructure-ics-scada-security-solutions-overview.pdf página 2** 	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

28	IPS debe tener un mecanismo para convertir firmas SNORT	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 195**	Verificado
29	La solución debe hacer cumplir la aplicación del protocolo Citrix	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 288, 289, 290**	Verificado
30	La solución debe permitir al administrador bloquear fácilmente el tráfico entrante y / o saliente en función de los países, sin la necesidad de administrar manualmente los rangos de IP correspondientes al país.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 165 "GEO Location"**	Verificado
31	El IPS debe permitir la captura de paquetes, para propósitos forenses, para firmas específicas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 186 – 187 packet capture**	Verificado
32	Adquisición de identidad de usuario	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **check-point-identity-awareness-datasheet.pdf**	Verificado
33	Debe poder adquirir la identidad del	**ENTERADOS,**	Ver **check-point-identity-awareness-datasheet.pdf página**	

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	usuario al consultar Microsoft Active Directory en función de los eventos de seguridad	**ACEPTAMOS Y CUMPLIMOS**		Verificado
34	La Solución debe ser capaz de adquirir la identidad de los usuarios, desde un directorio activo, sin la necesidad de instalar software/agentes en los controladores de dominio, basado en la lectura de los eventos de seguridad de Microsoft.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **check-point-identity-awareness-datasheet.pdf página 2 "Active Directory"**	Verificado
35	Debe tener un método de autenticación de identidad de usuario basado en navegador para usuarios o activos que no sean de dominio	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **check-point-identity-awareness-datasheet.pdf página 3 "Browser-Based Authentication"**	Verificado
36	Debe tener un agente de cliente dedicado que pueda instalarse por política en las computadoras de los usuarios que puedan adquirir e informar identidades a la pasarela de seguridad.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R80.40_IdentityAwareness_AdminGuide.pdf página 202,203,204,205,206,207**	Verificado
37	Debe tener soporte de Kerberos (Principalmente en Directorio Activo), para poder realizar procesos de autenticación transparente y garantizar Single Sign-On.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R80.40_IdentityAwareness_AdminGuide.pdf página 184,185**	Verificado

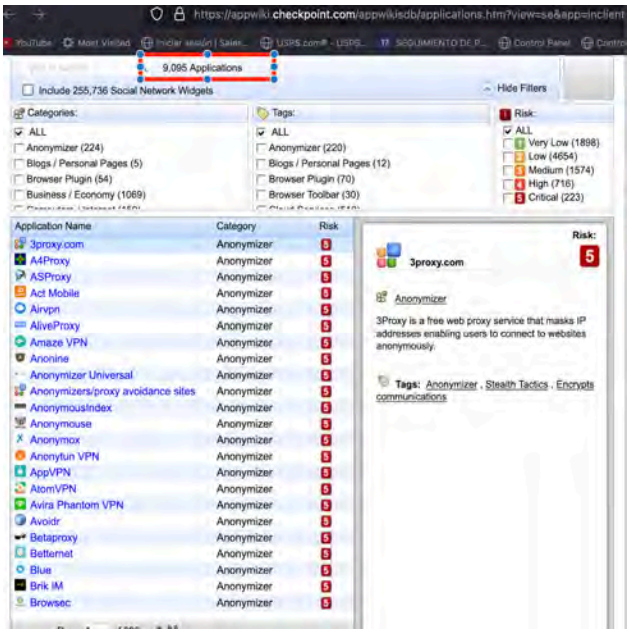
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

38	Debe soportar grupos anidados dentro del directorio activo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R80.40_IdentityAwareness_AdminGuide.pdf página 149, 150 "Nested Groups"**	Verificado
39	Debe admitir entornos de servidor de terminal	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **check-point-identity-awareness-datasheet.pdf página 2 "Terminal server"**	Verificado
40	La solución debe integrarse sin problemas con los servicios de directorio, IF-MAP y Radius	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R80.40_IdentityAwareness_AdminGuide.pdf página 241, 242, 33**	Verificado
41	La solución de identidad debe admitir servidores de terminal y citrix	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **check-point-identity-awareness-datasheet.pdf página 2 "Terminal server", "Citrix"**	Verificado
42	La solución debe permitir la identificación a través de un proxy (por ejemplo: encabezados X-forward)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R80.40_IdentityAwareness_AdminGuide.pdf página 47**	Verificado
43	Debe poder adquirir la identidad del usuario de Microsoft Active Directory sin ningún tipo de agente instalado en los controladores de dominio	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **check-point-identity-awareness-datasheet.pdf página 2 "Active Directory"**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

44	Debe admitir la autenticación transparente de Kerberos para el inicio de sesión único	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **check-point-identity-awareness-datasheet.pdf página 3 "Browser-Based Authentication"** Ver **CP_R80.40_IdentityAwareness_AdminGuide.pdf página 184,185**	Verificado
45	Debe admitir el uso de grupos anidados LDAP	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R80.40_IdentityAwareness_AdminGuide.pdf página 149, 150 "LDAP Nested Groups"**	Verificado
46	Debe poder compartir o propagar identidades de usuario entre múltiples puertas de enlace de seguridad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R80.40_IdentityAwareness_AdminGuide.pdf página 167** ▪ Large-scale enterprise deployment - In large networks, deploy multiple Security Gateway. For example: deploy a perimeter Firewall and multiple Data Centers. Install an identity-based policy on all Identity Awareness Security Gateway. The Identity Awareness Gateways share user and computer data of the complete environment.	Verificado
47	Debe poder crear roles de identidad para usar en todas las aplicaciones de seguridad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R80.40_IdentityAwareness_AdminGuide.pdf página 42**	Verificado
48	Control de aplicaciones y filtrado de URL	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución incluye control de aplicaciones y filtrado URL. **ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

49	La base de datos de control de aplicaciones debe contener más de 8000 aplicaciones conocidas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 3** **Applications** • Use 8,000+ pre-defined or customize your own applications 	Verificado
50	La solución debe ser capaz de crear una regla de filtrado con múltiples categorías	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R76/CP_R76_AppControl_WebAdmin/60902.htm “Site Category” “Multiple categories”	Verificado

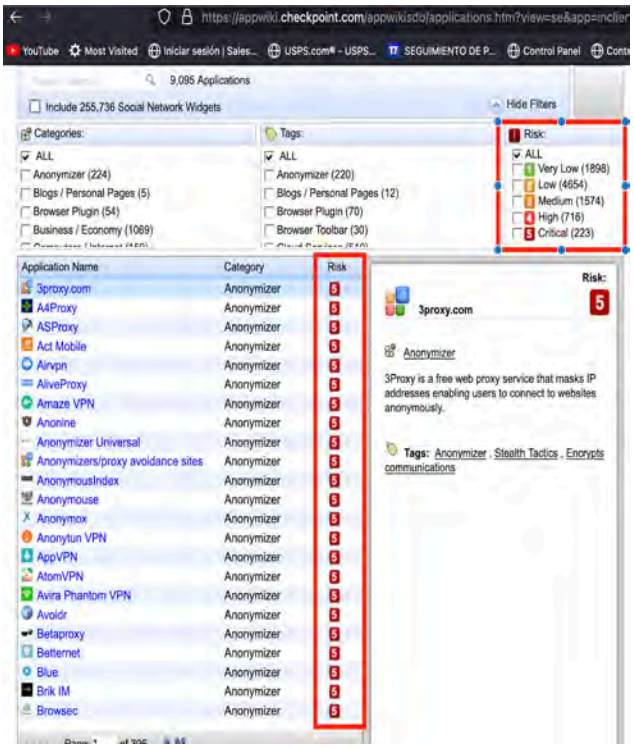
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			Site Category The Site Category column contains the categories for sites and applications that users browse to and you choose to include. One rule can include multiple categories of different types.	
51	La solución debe ser capaz de crear un filtro para un solo sitio que sea compatible con múltiples categorías.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 185, 186.** **Ver** https://sc1.checkpoint.com/documents/SMB_R80.20/AdminGuides/Locally_Managed/EN/Content/Topics/Managing-Applications-_-URLs.htm Each URL is inspected by the Check Point Cloud using the URL Filtering blade and can be matched to one or more built in categori sites, high bandwidth, gambling, or shopping, etc.).	Verificado
52	La solución debe tener granularidad de usuarios y grupos con reglas de seguridad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R76/CP_R76_AppControl_WebAdmin/60897.htm ▪ **Create a Granular Policy** Make rules to allow or block applications or internet sites, by individual application, application or URL categories, or risk levels. When you use Identity Awareness, you can easily make rules for individuals or different groups of users. You can also create an HTTPS Policy that enables the Security Gateway to inspect HTTPS traffic to prevent security risks related to the SSL protocol.	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			▪ **Custom Applications, Sites, Categories and Groups** You can create applications, websites, categories and groups that are not in the Application and URL Filtering Database for use in the Policy. Use these custom objects to create a Rule Base that meets your organization requirements. You can contact Check Point to create customized application signatures to be imported into the database. These signatures contain a database of internal applications that are not necessarily web-based. ▪ **Primary Category** - Group of applications with a common defining aspect. Each application has one primary category which is the most defining aspect of the application. See the category in the application descriptions and in the logs. When URL Filtering is enabled, categories also define a group of URLs or patterns of URLs. ▪ **Additional Categories** - Characteristics of the application. In the Application and URL Filtering Database, applications can have multiple categories. For example, Gmail categories include: Supports File Transfer, Sends mail, and Instant Chat. You can include categories in rules in the Rule Base. If a category is in a rule, the rule matches all applications and sites that are marked with that category. For example if you block the "Sends mail" category: Gmail, Yahoo! Mail, and others will be blocked.	
53	La solución debe tener una interfaz de búsqueda fácil de usar para aplicaciones y URL	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R76/CP_R76_AppControl_WebAdmin/60902.htm To add applications or categories to a rule: Put your mouse in the column and a plus sign shows. Click the plus sign to open the Application viewer. For each application or widget, the viewer shows a short description and its related categories. For each category, the viewer shows a description and if there are applications or sites related with it. • To add an item to the rule, click the checkbox in the **Available** list. • To see the details of an item without adding it to the rule, click the name of the **Available** item. • You can select an application, category, site or group to add to the rule from the **Available** list. • To filter the **Available** list by categories, applications, custom-defined items or widgets, click the buttons in the toolbar of the viewer. The Available list shows the filtered items and then you can add items to the rule. • To see all applications in a risk level, select the level from the **Risk** field in the toolbar. • If you know the name of an application or category, you can search for it. The results show in the **Available** list. • To add a new category, application or site, or application or site group, use the **New** button.	Verificado
54	La solución debe categorizar aplicaciones y URL y aplicaciones por Factor de riesgo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 199 “risk”**	Verificado

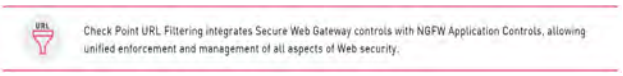
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

				
55	El control de la aplicación y la política de seguridad URLF deben poder definirse por las identidades del usuario	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	El control de aplicaciones y los filtros URL se pueden definir por las identidad del usuario, se puede aplicar políticas de control de navegación a usuario o grupo del directorio activo. Ver https://sc1.checkpoint.com/documents/R76/CP_R76_AppControl_WebAdmin/60897.htm	

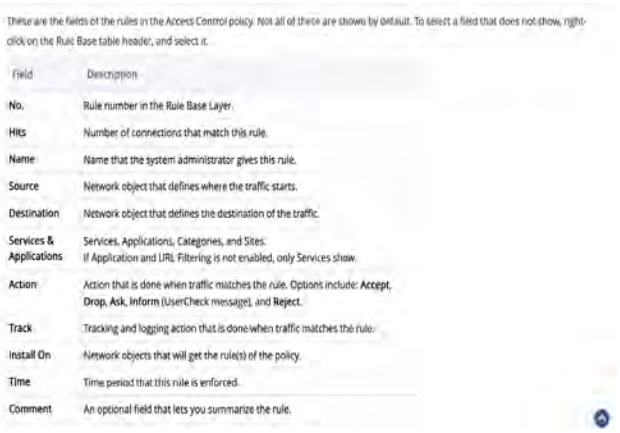
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			▪ **Create a Granular Policy** Make rules to allow or block applications or internet sites, by individual application, application or URL categories, or risk levels. When you use Identity Awareness, you can easily make rules for individuals or different groups of users. You can also create an HTTPS Policy that enables the Security Gateway to inspect HTTPS traffic to prevent security risks related to the SSL protocol. ▪ **Custom Applications, Sites, Categories and Groups** You can create applications, websites, categories and groups that are not in the Application and URL Filtering Database for use in the Policy. Use these custom objects to create a Rule Base that meets your organization requirements. You can contact Check Point to create customized application signatures to be imported into the database. These signatures contain a database of internal applications that are not necessarily web-based.	Verificado
56	El control de la aplicación y la base de datos URLF deben ser actualizados por un servicio basado en la nube	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R80/CP_R80_SmartDashboard_OLH/html_frameset.htm?topic=documents/R80/CP_R80_SmartDashboard_OLH/iaDFuGv6nracp6BbIVSzzw2 *Updating the Application and URL Filtering Database* The Application and URL Filtering Database on the Security Gateway gets regular, automatic updates that make sure that you have the most current data and newly added applications and websites in the Application and URL Filtering Layer of the Access Control Policy. By default, updates run on the Security Management Server and Security Gateways once a day. You can change the update schedule or choose to manually update the management server. The updates are stored in a few files on each Security Gateway. https://www.checkpoint.com/quantum/url-filtering/	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

57	La solución debe tener control unificado de la aplicación y reglas de seguridad URLF	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **Software-Blades-Architecture.pdf página 5**  	Verificado
58	La solución debe proporcionar un mecanismo para informar o pedir a los usuarios en tiempo real que los eduquen o confirmen acciones basadas en la política de seguridad.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	El modulo de filtro URL, dentro de sus reglas permite configurar una acción de informar al usuario en tiempo real del contenido o tipo de pagina en la que está intentado navegar de tal forma que se vaya educando acerca de en donde puede navegar y en donde no. Ver https://sc1.checkpoint.com/documents/R76/CP_R76_AppControl_WebAdmin/60902.htm  	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

59	La solución debe proporcionar un mecanismo para limitar el uso de la aplicación en función del consumo de ancho de banda	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 200,201**	Verificado
60	La solución debe permitir excepciones de red basadas en objetos de red definidos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución permite excepciones basada en objetos de red definidos, estos se configuran en los campos de origen, destino, servicio&aplicación, acción, etc. Ver https://sc1.checkpoint.com/documents/R80/CP_R80BC_ApplicationControlURLFiltering/html_frameset.htm 	Verificado

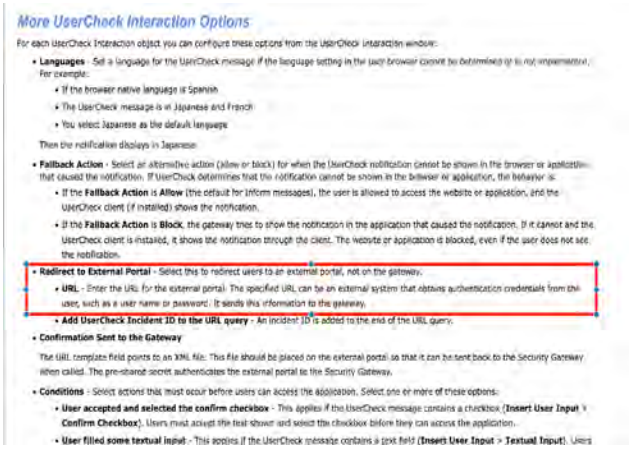
These are the fields of the rules in the Access Control policy. Not all of these are shown by default. To select a field that does not show, right-click on the Rule Base table header, and select it.

Field	Description
No.	Rule number in the Rule Base Layer.
Hits	Number of connections that match this rule.
Name	Name that the system administrator gives this rule.
Source	Network object that defines where the traffic starts.
Destination	Network object that defines the destination of the traffic.
Services & Applications	Services, Applications, Categories, and Sites. If Application and URL Filtering is not enabled, only Services show.
Action	Action that is done when traffic matches the rule. Options include: **Accept**, **Drop**, **Ask**, **Inform** (UserCheck message), and **Reject**.
Track	Tracking and logging action that is done when traffic matches the rule.
Install On	Network objects that will get the rule(s) of the policy.
Time	Time period that this rule is enforced.
Comment	An optional field that lets you summarize the rule.

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

61	La solución debe proporcionar la opción de modificar la Notificación de bloqueo y redirigir al usuario a una página de corrección.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R76/CP_R76_AppControl_WebAdmin/60902.htm **UserCheck Interaction Objects** UserCheck Interaction Objects add flexibility to Application and URL Filtering by giving the Security Gateway a mechanism to communicate with users. UserCheck objects are used in the Application and URL Filtering Rule Base to: • Help users with decisions that can be dangerous to the organization security. • Share the organization changing internet policy for web applications and sites with users, in real-time. If a UserCheck object is set as the action on a policy rule, the browser redirects to the web portal on port 443 or 80. The portal hosts UserCheck notifications. The UserCheck client adds the option to send notifications for applications that are not in a web browser, such as Skype, iTunes, or browser add-ons (such as radio toolbars). The UserCheck client can also work together with the UserCheck portal to show notifications on the computer itself when: • The notification cannot be displayed in a browser, or • The UserCheck engine determines that the notification will not be shown correctly in the browser and the **Fallback Action** for the UserCheck object is **Allow**. For more about configuring UserCheck on the gateway and the UserCheck client, see Configuring UserCheck. **Creating UserCheck Interaction Objects** Create a UserCheck Interaction object from the Rule Base or from the **UserCheck** page of the Application and URL Filtering tab. The procedure below shows how to create the object from the Rule Base. To create a UserCheck object that includes a message: 1. In the **Application & URL Filtering** > **Policy** rule base > **Action** column, select one of these interaction modes: • **Inform** - Show an informative message users. Users can continue to the application or cancel the request. • **Ask** - Show a message to users that asks them if they want to continue with the request or not. • **Block** - Show a message to users and block the application request. 2. Select **New UserCheck** or one of the existing UserCheck Interaction objects. If you selected **New UserCheck**, the **UserCheck Interaction** window opens on the **Message** page. 3. Enter a name for the UserCheck object and, optionally, a comment. 4. Select a language (English is the default) from the **Languages** tabs. 5. Click the **Add logo** box to add a graphic, such as company logo. **Note** - The graphic must have a height and width of 176 x 52 pixels. 6. Click the text box adjacent to the picture and enter title text for the message. **Note** - Right-clicking inside any of the text boxes gives you the option to Switch to HTML mode and enter HTML code directly. Switching to HTML mode closes the formatting toolbar. 7. In the page title, message subject, and message body text boxes, enter the message content. You can: 1. Use the formatting toolbar to change text color, alignment, add or remove bullets. 2. **Insert field** variables for: ◦ Application name ◦ Category	Verificado

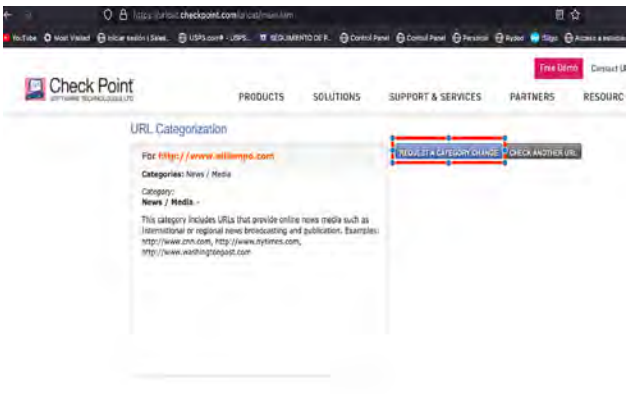
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

				
62	La solución debe incluir un mecanismo de listas en blanco y negro que permita al administrador denegar o permitir URL específicas independientemente de la categoría	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución de filtrado URL cuenta con un mecanismo a traves del cual se pueden crear listados de URLs, y aplicarlos a las reglas de filtrado configurando una acción de permitir o denegar la navegación hacia dichas URLs independientemente de las categorías, permitiendo crear listas blancas y listas negras. Ver https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk103051 Ver **CP_ApplicationControlSignatureTool_AdminGuide.pdf** Ver	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			 https://sc1.checkpoint.com/documents/R76/CP_R76_AppControl_WebAdmin/60902.htm	
63	La solución debe tener un mecanismo de bypass configurable	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R76/CP_R76_AppControl_WebAdmin/60902.htm 	Verificado
64	La solución debe proporcionar un	**ENTERADOS,**		

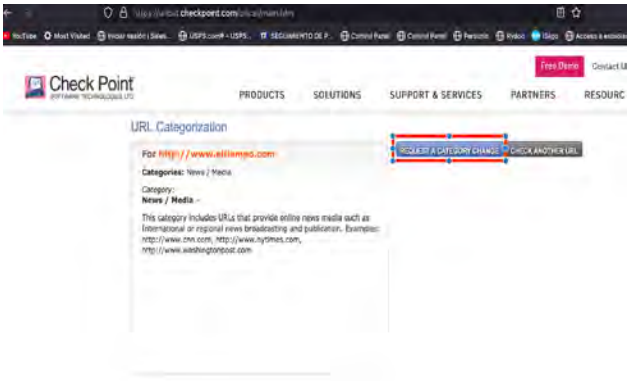
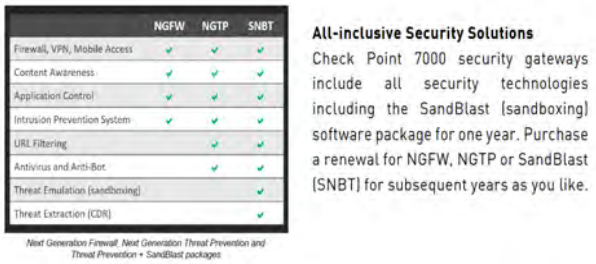
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	mecanismo de anulación en la categorización de la base de datos de URL	**ACEPTAMOS Y CUMPLIMOS**	La solución cuenta con un mecanismo a traves de una herramienta de recategorización de URLs y un procedimiento de anulación de la categorización. https://urlcat.checkpoint.com/urlcat/main.htm  https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk92941 Adicionalmente cuanta con un mecanismo de Fail-mode, en caso de que el motor de filtrado falle puede anular la categorización, es decir permitir o bloquear toda la navegación. https://sc1.checkpoint.com/documents/R80/CP_R80_SmartDashboard_OLH/html_frameset.htm?topic=documents/R80/CP_R80_SmartDashboard_OLH/7IwBkYZnE5dyeAqAU5ILiA2	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			"Fail-Mode" *Fail Mode* You can select the enforcement option to use if the Application and URL Filtering engine fails during inspection. To select the enforcement option 1. Go to **Manage & Settings** > **blades** > **Application and URL Filtering** > **Advanced Settings**. 2. In the **Application Settings** window, select one option: • **Allow all requests (fail-open) -** All traffic is allowed. • **Block all requests (fail-close)** - All traffic is blocked (default). *Web Browsing* If you do not enable URL Filtering on the Security Gateway, you can use a generic Web browser application called **Web Browsing** in the rule. This application includes all HTTP traffic that is not a defined application. Because Web Browsing traffic can generate many logs, the Web browsing application has its own activation setting. Application and URL Filtering assigns **Web Browsing** as the default application for all HTTP traffic that does not match an application in the Application and URL Filtering Database. The **Web Browsing** application is activated by default. If you deactivate the Web browsing application: • **Web Browsing** in Access Control Policy rules is not enforced. For example, if you have a rule that blocks **Web Browsing**, traffic is allowed. • No **Web Browsing** logs are generated. To deactivate the Web Browsing application: 1. Go to **Manage & Settings** > **blades** > **Application and URL Filtering** > **Advanced Settings**. 2. Deselect **Enable web browsing logging and policy enforcement**.	
65	El control de la aplicación y la política de seguridad URLF deben informar sobre el recuento de aciertos de la regla	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 229,230**	Verificado
66	La Solución debe proveer un mecanismo que permita re-categorizar los sitios WEB.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución cuenta con un mecanismo a traves de una herramienta de recategorización de URLs. https://urlcat.checkpoint.com/urlcat/main.htm	

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

				Verificado
C	**Anti-Bot y Anti-Virus**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	
1	El proveedor debe tener una aplicación integrada Anti-Bot y Anti-Virus en el firewall de próxima generación	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 2 (Antivirus and Anti-bot)**  *Next Generation Firewall, Next Generation Threat Prevention and Threat Prevention + SandBlast packages*	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

2	La aplicación anti-bot debe ser capaz de detectar y detener el comportamiento anormal sospechoso de la red	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 29** Ver **ds-anti-bot.pdf**	Verificado
3	La aplicación Anti-Bot debe usar un motor de detección de múltiples niveles, que incluye la reputación de direcciones IP, URL y DNS, y detectar patrones de comunicaciones de bots.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **ds-anti-bot.pdf página 1, 2** Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 29**	Verificado
4	Las protecciones anti-Bot deben poder escanear en busca de acciones de bots	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **ds-anti-bot.pdf página 1, 2** Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 29**	Verificado
5	La solución debe ser compatible con la detección y prevención de virus y variantes de Cryptors y ransomware (p. Ej., Wannacry, Cryptlocker, CryptoWall ...) mediante el uso de análisis estáticos y / o dinámicos.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución es compatible con la detección y prevención de amenazas de Cryptors y ransomware a traves de las tecnologías de SandBlast, mediante el análisis estático y dinámico. Ver **preventing-wannacry-ransomware-and-zero-day-attacks.pdf** Ver https://blog.checkpoint.com/2017/05/12/global-outbreak-wanacryptor/	Verificado
6	La solución debe tener mecanismos para proteger contra	**ENTERADOS, ACEPTAMOS Y**		

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	los ataques de spear phishing	**CUMPLI MOS**	La solución permite proteger contra ataques de spear phishing a traves del modulo de SandBlast. https://blog.checkpoint.com/2016/05/20/spear-phishing-2-0-adds-social-engineering-vm-evasion/	Verificado
7	El componente de control de Bots, debe ser capaz de detectar y prevenir ataques tipo ransomware y sus variantes (ej. Wannacry, Cryptolocker, CryptoWall) a través de análisis, estático o dinámico.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver https://blog.checkpoint.com/2017/05/12/global-outbreak-wanacryptor/	Verificado
8	Ataques basados en DNS:	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 85, 86**	Verificado
D	La solución debe tener capacidades de detección y prevención para los escondites DNS de C & C.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver **ds-anti-bot.pdf página 1, 2**	Verificado
1	Búsqueda de patrones de tráfico C & C, no solo en su destino DNS	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver Ver **ds-anti-bot.pdf página 1, 2**	Verificado
2	Ingeniería reversa del malware para descubrir su DGA (Domain name generation)	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver	Verificado

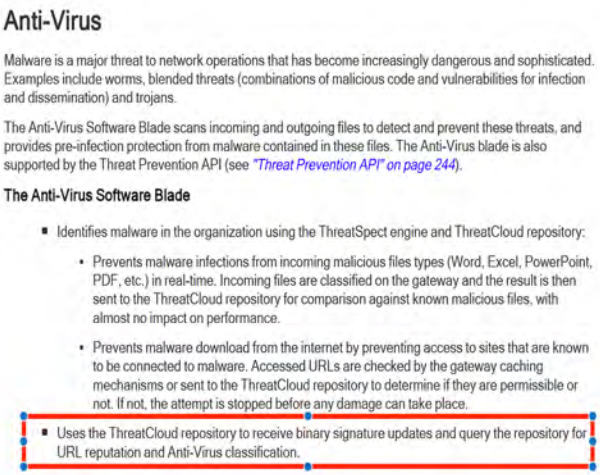
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			https://blog.checkpoint.com/2013/11/14/defeating-cryptolocker-with-threatcloud-and-gateway-threat-prevention/	
3	Característica de captura DNS como parte de la prevención de amenazas, ayudando a descubrir hosts infectados generando comunicación C & C	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **ds-anti-bot.pdf páginas 1, 2** 	Verificado
4	La solución debe detectar comunicaciones hacia sitios de comando & control, basados entre otros en direcciones IP, URL & Reputación de Dominios.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **ds-anti-bot.pdf páginas 1, 2**	Verificado
5	La solución debe contar con la capacidad de detectar & prevenir ataques encapsulados en túneles DNS.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://www.checkpoint.com/cyber-hub/network-security/what-is-dns-security/	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			Check Point solutions can help organizations protect DNS infrastructure and detect DNS-based attacks. Next-Gen Firewalls detect malicious traffic and DNS tunneling attacks via Reputation filtering and IPS DNS Tunneling protections. In addition we can empower SOC teams to research IoCs and find look alike domains to protect against cyber threats such as those exploiting DNS in phishing attacks. Check out this demo of Check Point Infinity SOC.	
6	La política de Anti-Bot y Anti-Virus debe administrarse desde una consola central	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución cuenta con una consola de administración centralizada desde la cual se administran centralizadamente todas las políticas de Anti-bot y Anti-virus. Ver **smart-1-security-management-platform-datasheet.pdf página 1**	Verificado
7	La aplicación Anti-Bot y Anti-Virus debe tener un mecanismo centralizado de correlación e informe de eventos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución cuenta con un módulo de reporte llamado SmartEventel cual permite tola correlación e informes de eventos. Ver **smartevent-datasheet.pdf páginas 1-4**	Verificado
8	La aplicación antivirus debe poder evitar el acceso a sitios web maliciosos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 30** **Anti-Virus** Malware is a major threat to network operations that has become increasingly dangerous and sophisticated. Examples include worms, blended threats (combinations of malicious code and vulnerabilities for infection and dissemination) and trojans. The Anti-Virus Software Blade scans incoming and outgoing files to detect and prevent these threats, and provides pre-infection protection from malware contained in these files. The Anti-Virus blade is also supported by the Threat Prevention API (see *"Threat Prevention API" on page 244*). **The Anti-Virus Software Blade** ▪ Identifies malware in the organization using the ThreatSpect engine and ThreatCloud repository: • Prevents malware infections from incoming malicious files types (Word, Excel, PowerPoint, PDF, etc.) in real-time. Incoming files are classified on the gateway and the result is then sent to the ThreatCloud repository for comparison against known malicious files, with almost no impact on performance. • Prevents malware download from the internet by preventing access to sites that are known to be connected to malware. Accessed URLs are checked by the gateway caching mechanisms or sent to the ThreatCloud repository to determine if they are permissible or not. If not, the attempt is stopped before any damage can take place. ▪ Uses the ThreatCloud repository to receive binary signature updates and query the repository for URL reputation and Anti-Virus classification.	Verificado
9	La aplicación antivirus debe poder inspeccionar el tráfico cifrado SSL	**ENTERADOS, ACEPTAMOS Y**	Ver	Verificado

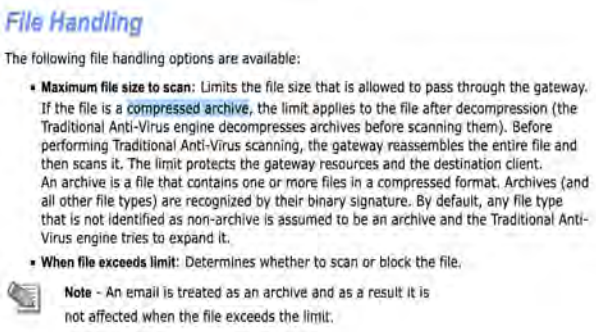
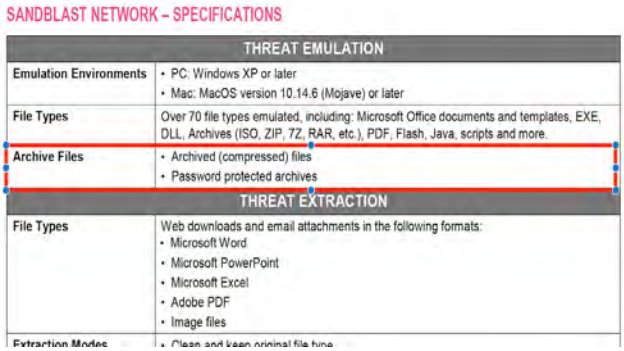
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS	https://www.checkpoint.com/cyber-hub/network-security/what-is-ssl-inspection/	
10	Anti-Bot y Anti-Virus deben tener actualizaciones en tiempo real de servicios de reputación basados en la nube	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 30**  Anti-Virus Malware is a major threat to network operations that has become increasingly dangerous and sophisticated. Examples include worms, blended threats (combinations of malicious code and vulnerabilities for infection and dissemination) and trojans. The Anti-Virus Software Blade scans incoming and outgoing files to detect and prevent these threats, and provides pre-infection protection from malware contained in these files. The Anti-Virus blade is also supported by the Threat Prevention API (see *"Threat Prevention API" on page 244*). **The Anti-Virus Software Blade** ▪ Identifies malware in the organization using the ThreatSpect engine and ThreatCloud repository: • Prevents malware infections from incoming malicious files types (Word, Excel, PowerPoint, PDF, etc.) in real-time. Incoming files are classified on the gateway and the result is then sent to the ThreatCloud repository for comparison against known malicious files, with almost no impact on performance. • Prevents malware download from the internet by preventing access to sites that are known to be connected to malware. Accessed URLs are checked by the gateway caching mechanisms or sent to the ThreatCloud repository to determine if they are permissible or not. If not, the attempt is stopped before any damage can take place. ▪ Uses the ThreatCloud repository to receive binary signature updates and query the repository for URL reputation and Anti-Virus classification. **https://threatmap.checkpoint.com/**	Verificado
11	Anti-Virus debe ser capaz de detener los archivos maliciosos entrantes	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 30**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			Anti-Virus Malware is a major threat to network operations that has become increasingly dangerous and sophisticated. Examples include worms, blended threats (combinations of malicious code and vulnerabilities for infection and dissemination) and trojans. The Anti-Virus Software Blade scans incoming and outgoing files to detect and prevent these threats, and provides pre-infection protection from malware contained in these files. The Anti-Virus blade is also supported by the Threat Prevention API (see *"Threat Prevention API" on page 244*). **The Anti-Virus Software Blade** ▪ Identifies malware in the organization using the ThreatSpect engine and ThreatCloud repository: • Prevents malware infections from incoming malicious files types (Word, Excel, PowerPoint, PDF, etc.) in real-time. Incoming files are classified on the gateway and the result is then sent to the ThreatCloud repository for comparison against known malicious files, with almost no impact on performance. • Prevents malware download from the internet by preventing access to sites that are known to be connected to malware. Accessed URLs are checked by the gateway caching mechanisms or sent to the ThreatCloud repository to determine if they are permissible or not. If not, the attempt is stopped before any damage can take place. ▪ Uses the ThreatCloud repository to receive binary signature updates and query the repository for URL reputation and Anti-Virus classification.	
12	El antivirus debe ser capaz de escanear archivos descargados.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_ThreatPrevention_AdminGuide.pdf página 30** **Anti-Virus** Malware is a major threat to network operations that has become increasingly dangerous and sophisticated. Examples include worms, blended threats (combinations of malicious code and vulnerabilities for infection and dissemination) and trojans. The Anti-Virus Software Blade scans incoming and outgoing files to detect and prevent these threats, and provides pre-infection protection from malware contained in these files. The Anti-Virus blade is also supported by the Threat Prevention API (see *"Threat Prevention API" on page 244*). **The Anti-Virus Software Blade** ▪ Identifies malware in the organization using the ThreatSpect engine and ThreatCloud repository: • Prevents malware infections from incoming malicious files types (Word, Excel, PowerPoint, PDF, etc.) in real-time. Incoming files are classified on the gateway and the result is then sent to the ThreatCloud repository for comparison against known malicious files, with almost no impact on performance. • Prevents malware download from the internet by preventing access to sites that are known to be connected to malware. Accessed URLs are checked by the gateway caching mechanisms or sent to the ThreatCloud repository to determine if they are permissible or not. If not, the attempt is stopped before any damage can take place. ▪ Uses the ThreatCloud repository to receive binary signature updates and query the repository for URL reputation and Anti-Virus classification.	Verificado
13	El antivirus será capaz de inspeccionar trafico pasando por el protocolo CIFS (carpetas compartidas), entre vlans de servidores y usuarios.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk101606	Verificado

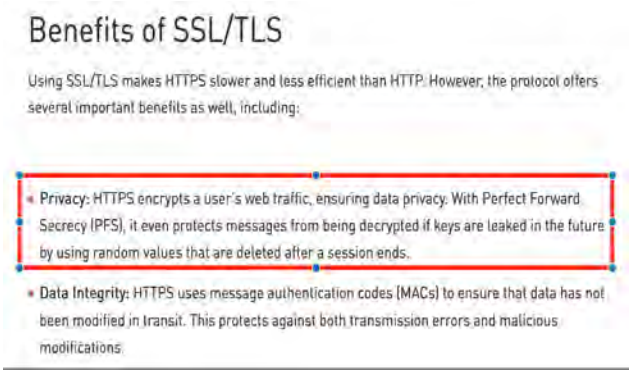
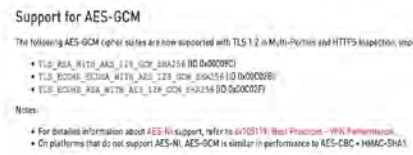
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

14	Anti-Virus debe poder escanear archivos de almacenamiento	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R77/CP_R77_ThreatPrevention_WebAdmin/101647.htm  Ver **sandblast-network-solution-brief.pdf página 5**  	Verificado
15	Las políticas de antivirus y anti-Bot se deben administrar de forma centralizada con la configuración de políticas granulares y la aplicación	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución cuenta con una consola de administración centralizada desde la cual se administran centralizadamente todas las políticas de Anti-bot y Anti-virus. Ver **smart-1-security-management-platform-datasheet.pdf página 1**	Verificado

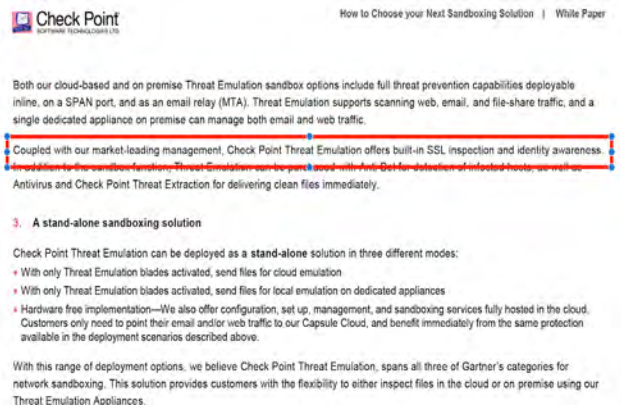
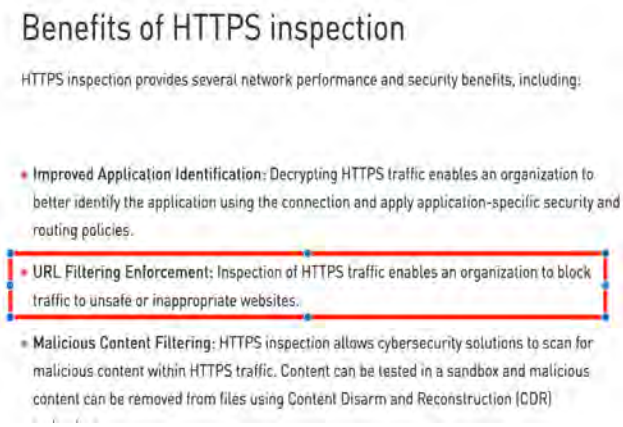
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

16	El Anti-Virus debería ser compatible con el escaneo de enlaces dentro de correos electrónicos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_ThreatPrevention_AdminGuide/138634 *Configuring Inspection of Links Inside Mail* **Inspection of Links Inside Mail** scans URL links in email messages. **Inspection of Links Inside Mail** is on by default, and is supported with the Anti-Virus, Anti-Bot and Threat Emulation blades. **Inspection of Links Inside Mail** scans incoming mail with the Anti-Virus Software Blade and outgoing mail with Anti-Bot Software Blade. For the Threat Emulation blade, only URL links to files are scanned. You must enable MTA for Inspection of Links Inside Mail to work with the Threat Emulation blade. On this page, you can configure these settings: • **Inspect first** <number> **(B) of email messages** • **Inspect first** <number> **URLs in email messages**	Verificado
17	El Anti-Virus debe Escanear archivos que están pasando el protocolo CIFS	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk101606	Verificado
E	**Inspección SSL (entrante / saliente)**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://www.checkpoint.com/cyber-hub/network-security/what-is-ssl-inspection/	Verificado
1	La solución ofrece soporte para la inspección / descifrado SSL con un rendimiento líder en todas las tecnologías de	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://www.checkpoint.com/cyber-hub/network-security/what-is-ssl-inspection/	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	mitigación de amenazas			
2	La solución debería ser compatible con Perfect Forward Secrecy (PFS)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://www.checkpoint.com/cyber-hub/network-security/what-is-ssl-inspection/ 	Verificado
3	La solución debe ser compatible con AES-NI, AES-GCM para mejorar el rendimiento	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk104717 	Verificado
4	La emulación de amenazas / sandboxing debe	**ENTERADOS, ACEPTA**	Ver **check-point-gartner-how-to-choose-sandboxing-solution-whitepaper.pdf página 2**	

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	integrarse con SSL Inspection	**MOS Y CUMPLI MOS**		Verificado
5	La solución debe aprovechar la base de datos de filtrado de URL para permitir al administrador crear una política de inspección https granular	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver https://www.checkpoint.com/cyber-hub/network-security/what-is-ssl-inspection/ 	Verificado
6	La solución puede inspeccionar el filtrado de URL basado en HTTPS sin necesidad de descifrado SSL	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk104717	Verificado

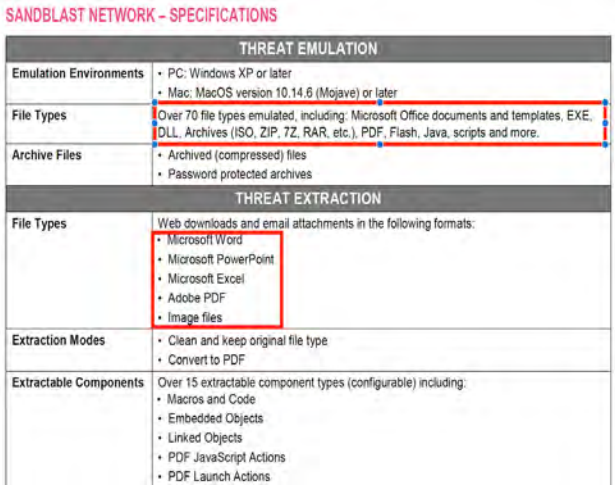
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			https://www.checkpoint.com/cyber-hub/network-security/what-is-ssl-inspection/	
F	**Emulación de amenazas (sandboxing)**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	
1	La solución debe proporcionar la capacidad de proteger contra ataques de malware desconocidos y de día cero antes de que se hayan creado protecciones de firmas estáticas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **sandblast-network-solution-brief.pdf página 1**	Verificado
2	1 Real-Time Prevention-unknown malware patient-0 en la navegación web	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://www.checkpoint.com/es/pages/gen-v-cyber-security/ https://www.checkpoint.com/comparison/check-point-vs-pan/ “Paciente 0”	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

				
3	1 Real-Time Prevention-unknown malware patient-0 en el correo electrónico	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://www.checkpoint.com/es/pages/gen-v-cyber-security/ https://www.checkpoint.com/comparison/check-point-vs-pan/ “Paciente 0” 	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

4	La solución debe actuar en modo prevención, en caso de malware de "paciente-0" (cero) en los procesos de navegación.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://www.checkpoint.com/es/pages/gen-v-cyber-security/ “Paciente 0” 	Verificado
5	La solución debe tener la capacidad de emular archivos Office (doc, docx, ppt, pptx, dot, xls,) archivos de empaquetamiento (tar, 7z, zip, gz)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **sandblast-network-solution-brief.pdf página 5** 	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

<table>
<tr><th>G</th><th>Protocolos</th><th>ENTERADOS, ACEPTAMOS Y CUMPLIMOS</th><th>ENTERADOS, ACEPTAMOS Y CUMPLIMOS</th><th></th></tr>
<tr><td>1</td><td>La solución debería ser capaz de emular ejecutable, archivar archivos, documentos, JAVA y flashear específicamente dentro de varios protocolos:</td><td>ENTERADOS, ACEPTAMOS Y CUMPLIMOS</td><td>Ver sandblast-network-solution-brief.pdf página 5

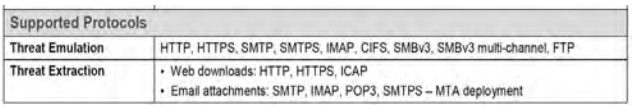
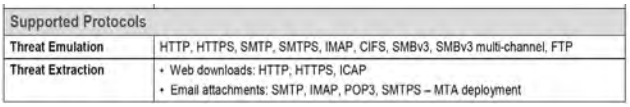
SANDBLAST NETWORK – SPECIFICATIONS
<table><tr><th colspan="2">THREAT EMULATION</th></tr><tr><td>Emulation Environments</td><td>• PC: Windows XP or later
• Mac: MacOS version 10.14.6 (Mojave) or later</td></tr><tr><td>File Types</td><td>Over 70 file types emulated, including: Microsoft Office documents and templates, EXE, DLL, Archives (ISO, ZIP, 7Z, RAR, etc.), PDF, Flash, Java, scripts and more.</td></tr><tr><td>Archive Files</td><td>• Archived (compressed) files
• Password protected archives</td></tr><tr><th colspan="2">THREAT EXTRACTION</th></tr><tr><td>File Types</td><td>Web downloads and email attachments in the following formats:
• Microsoft Word
• Microsoft PowerPoint
• Microsoft Excel
• Adobe PDF
• Image files</td></tr><tr><td>Extraction Modes</td><td>• Clean and keep original file type
• Convert to PDF</td></tr><tr><td>Extractable Components</td><td>Over 15 extractable component types (configurable) including:
• Macros and Code
• Embedded Objects
• Linked Objects
• PDF JavaScript Actions
• PDF Launch Actions</td></tr></table></td><td>Verificado</td></tr>
<tr><td>2</td><td>HTTP</td><td>ENTERADOS, ACEPTAMOS Y CUMPLIMOS</td><td>Ver sandblast-network-solution-brief.pdf página 5

<table><tr><th colspan="2">Supported Protocols</th></tr><tr><td>Threat Emulation</td><td>HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, SMBv3 multi-channel, FTP</td></tr><tr><td>Threat Extraction</td><td>• Web downloads: HTTP, HTTPS, ICAP
• Email attachments: SMTP, IMAP, POP3, SMTPS – MTA deployment</td></tr></table></td><td>Verificado</td></tr>
<tr><td>3</td><td>HTTPS</td><td>ENTERADOS, ACEPTAMOS Y CUMPLIMOS</td><td>Ver sandblast-network-solution-brief.pdf página 5</td><td></td></tr>
</table>

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			<table><tr><th colspan="2">Supported Protocols</th></tr><tr><td>Threat Emulation</td><td>HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, SMBv3 multi-channel, FTP</td></tr><tr><td>Threat Extraction</td><td>• Web downloads: HTTP, HTTPS, ICAP • Email attachments: SMTP, IMAP, POP3, SMTPS – MTA deployment</td></tr></table>	Verificado
4	SMTP	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **sandblast-network-solution-brief.pdf página 5** <table><tr><th colspan="2">Supported Protocols</th></tr><tr><td>Threat Emulation</td><td>HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, SMBv3 multi-channel, FTP</td></tr><tr><td>Threat Extraction</td><td>• Web downloads: HTTP, HTTPS, ICAP • Email attachments: SMTP, IMAP, POP3, SMTPS – MTA deployment</td></tr></table>	Verificado
5	SMTP TLS	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **sandblast-network-solution-brief.pdf página 5** **SMTPS** <table><tr><th colspan="2">Supported Protocols</th></tr><tr><td>Threat Emulation</td><td>HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, SMBv3 multi-channel, FTP</td></tr><tr><td>Threat Extraction</td><td>• Web downloads: HTTP, HTTPS, ICAP • Email attachments: SMTP, IMAP, POP3, SMTPS – MTA deployment</td></tr></table>	Verificado
6	PO3	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Se refiere al protocolo POP3, modificado por adenda. Ver **sandblast-network-solution-brief.pdf página 5** <table><tr><th colspan="2">Supported Protocols</th></tr><tr><td>Threat Emulation</td><td>HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, SMBv3 multi-channel, FTP</td></tr><tr><td>Threat Extraction</td><td>• Web downloads: HTTP, HTTPS, ICAP • Email attachments: SMTP, IMAP, POP3, SMTPS – MTA deployment</td></tr></table>	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

7	FTP	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **sandblast-network-solution-brief.pdf página 5**  Supported Protocols Threat Emulation: HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, SMBv3 multi-channel, FTP Threat Extraction: • Web downloads: HTTP, HTTPS, ICAP • Email attachments: SMTP, IMAP, POP3, SMTPS – MTA deployment	Verificado
8	CIFS (SMB)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **sandblast-network-solution-brief.pdf página 5**  Supported Protocols Threat Emulation: HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, SMBv3 multi-channel, FTP Threat Extraction: • Web downloads: HTTP, HTTPS, ICAP • Email attachments: SMTP, IMAP, POP3, SMTPS – MTA deployment	Verificado
H	**Tecnología Sandboxing:**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	
1	El motor de emulación debería poder inspeccionar, emular, prevenir y compartir los resultados del evento de sandboxing en la infraestructura antimalware	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_ThreatPrevention_AdminGuide.pdf página 32	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			Assigning Administrators for Threat Prevention You can control the administrator Threat Prevention permissions with a customized Permission Profile. The customized profile can have different Read/Write permissions for Threat Prevention policy, settings, profiles and protections. **Analyzing Threats** Networks today are more exposed to cyber-threats than ever. This creates a challenge for organizations in understanding the security threats and assessing damage. SmartConsole helps the security administrator find the cause of cyber-threats, and remediate the network. The Logs & Monitor > **Logs** view presents the threats as logs. The other views in the Logs & Monitor view combine logs into meaningful security events. For example, malicious activity that occurred on a host in the network in a selected time interval (the last hour, day, week or month). They also show pre- and post-infections statistics. You can create rich and customizable views and reports for log and event monitoring, which inform key stakeholders about security activities. For each log or event, you can see a lot of useful information from the ThreatWiki and IPS Advisories about the malware, the virus or the attack.	
2	La solución debería poder realizar un filtrado estático previo a la emulación	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver check-point-gartner-how-to-choose-sandboxing-solution-whitepaper.pdf 2. ***"Static analysis and other pre-filtering techniques[8]"*** Check Point offers a multi-layered threat prevention strategy, using IPS, Antivirus, Anti-Bot, OS-level Threat Emulation, CPU-level Threat Emulation, Threat Extraction, and Threat Intelligence. Our IPS, Antivirus, and Anti-Bot solutions help filter out known threats, while Threat Emulation and Threat Extraction provide protection against new and unknown threats. Check Point leverages multiple pre-emulation engines to minimize the number of objects sent to the sandbox. We utilize advanced machine learning engines for executable files and various signature-based Antivirus engines. Static analysis evaluates and identifies malware without requiring sandbox analysis. In addition, we reduce sandboxing sessions by caching files sent through multiple channels of attack on the gateways, on the Threat Emulation appliance and on the cloud service. As new threats are confirmed as malware, updates are provided to static filtering engines in real-time.	Verificado
3	la solución permitiría la emulación de archivos con un tamaño superior a 10 Mb en todos los tipos que admita	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 3**	Verificado

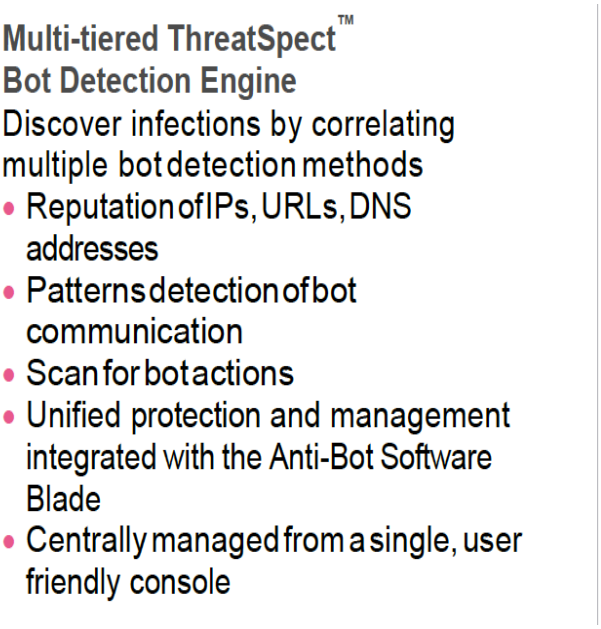
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			Content Security **First Time Prevention Capabilities** • CPU-level, OS-level and static file analysis • File disarm and reconstruction via Threat Extraction • Average emulation time for unknown files that require full sandbox evaluation is under 100 seconds • Maximal file size for Emulation is 100 MB • Emulation OS Support: Windows XP, 7, 8.1, 10	
4	Las soluciones deberían ser compatibles con los motores de detección basados en el aprendizaje automático de máquinas	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver check-point-gartner-how-to-choose-sandboxing-solution-whitepaper.pdf 2. ***"Static analysis and other pre-filtering techniques[6]"*** Check Point offers a multi-layered threat prevention strategy, using IPS, Antivirus, Anti-Bot, OS-level Threat Emulation, CPU-level Threat Emulation, Threat Extraction, and Threat Intelligence. Our IPS, Antivirus, and Anti-Bot solutions help filter out known threats, while Threat Emulation and Threat Extraction provide protection against new and unknown threats. Check Point leverages multiple pre-emulation engines to minimize the number of objects sent to the sandbox. We utilize advanced machine learning engines for executable files and various signature-based Antivirus engines. Static analysis evaluates and identifies malware without requiring sandbox analysis. In addition, we reduce sandboxing sessions by caching files sent through multiple channels of attack on the gateways, on the Threat Emulation appliance and on the cloud service. As new threats are confirmed as malware, updates are provided to static filtering engines in real-time.	Verificado
5	La solución debe detectar el ataque en la etapa de explotación, es decir, antes de que se ejecute el código de shell y antes de que se descargue / ejecute el malware.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **sandblast-network-solution-brief.pdf** **check-point-gartner-how-to-choose-sandboxing-solution-whitepaper.pdf**	Verificado
6	La solución debe ser capaz de detectar ROP y otras técnicas de explotación (por ejemplo, escalada de privilegios) mediante el control del flujo de la CPU	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver ROP https://blog.checkpoint.com/2016/06/22/intel-spot-on-with-cet/ **sandblast-network-solution-brief.pdf página 1**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			check-point-gartner-how-to-choose-sandboxing-solution-whitepaper.pdf página 2	
7	La solución debe ser capaz de admitir enlaces de escaneo dentro de correos electrónicos de 0 días y malware desconocido.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **sandblast-network-solution-brief.pdf página 1,2,3**	Verificado
8	La solución de emulación de amenazas debe permitir la 'Restricción geográfica' que permite que las emulaciones se restrinjan a un país específico.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97877	Verificado
9	La solución debe proporcionar la capacidad de Incrementar la seguridad con el intercambio automático de nueva información de ataque con otras pasarelas en forma de actualizaciones de firmas, etc.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	CP_R81_ThreatPrevention_AdminGuide.pdf página 31 When emulation is done on a file ▪ The file is opened on more than one virtual computer with different operating system environments. ▪ The virtual computers are closely monitored for unusual and malicious behavior, such as an attempt to change registry keys or run an unauthorized process. ▪ Any malicious behavior is immediately logged and you can use Prevent mode to block the file from the internal network. ▪ The cryptographic hash of a new malicious file is saved to a database and the internal network is protected from that malware. ▪ After the threat is caught, a signature is created for the new (previously unknown) malware which turns it into a known and documented malware. The new attack information is automatically shared with Check Point ThreatCloud to block future occurrences of similar threats at the gateway.	Verificado
10	El motor de emulación debe superar el 90% de tasa de captura en las pruebas de Virus Total donde los archivos PDF y exe maliciosos conocidos se modifican con encabezados "no	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **300TestReport.pdf**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	utilizados" para demostrar la capacidad de las soluciones para detectar malware nuevo y desconocido			
11	La solución debe detectar el tráfico de C & C de acuerdo con la reputación dinámica de ip / url	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver ds-anti-bot.pdf página 1 	Verificado
12	La solución debería ser capaz de emular y extraer archivos incrustados en documentos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-sandboxing/	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			To maintain business productivity, Check Point's threat emulation is used in combination with threat extraction to provide a seamless experience for the user. Threat Extraction cleans PDFs, images and other documents, removing exploitable elements such as active content and embedded objects. Files are then reconstructed, retaining their original format, and delivered to the user. Meanwhile, the original file is emulated in the background, and can be accessed by the user if deemed benign.	
13	La solución debe poder escanear documentos que contienen URL	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_ThreatPrevention_AdminGuide.pdf página 32 ▪ PDF documents with • Actions such as launch, sound, or movie URIs • JavaScript actions that run code in the reader's Java interpreter • Submit actions that transmit the values of selected fields in a form to a specified URL • Incremental updates that keep earlier versions of the document • Document statistics that show creation and modification dates and changes to hyperlinks • Summarized lists of properties	Verificado
I	**Detección de actividad del sistema:**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	
1	**La solución debe monitorear la actividad sospechosa en:**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Verificado
2	Llamadas API	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Todas estas técnicas de monitoreo de actividad sospechosa son propias de la solución de sandboxing de Checkpoint. Ver https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			Ver SandBlast Now - v12.pdf página 17	
3	Cambios del sistema de archivos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Todas estas técnicas de monitoreo de actividad sospechosa son propias de la solución de sandboxing de Checkpoint. Ver https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/ Ver SandBlast Now - v12.pdf página 17	Verificado
4	Registro del sistema	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Todas estas técnicas de monitoreo de actividad sospechosa son propias de la solución de sandboxing de Checkpoint. Ver https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/ Ver SandBlast Now - v12.pdf página 17	Verificado
5	Conexiones de red	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Todas estas técnicas de monitoreo de actividad sospechosa son propias de la solución de sandboxing de Checkpoint. Ver https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/ Ver SandBlast Now - v12.pdf página 17	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

6	Procesos del sistema	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Todas estas técnicas de monitoreo de actividad sospechosa son propias de la solución de sandboxing de Checkpoint. Ver https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/ Ver SandBlast Now - v12.pdf página 17	Verificado
7	Creación y eliminación de archivos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Todas estas técnicas de monitoreo de actividad sospechosa son propias de la solución de sandboxing de Checkpoint. Ver https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/ Ver SandBlast Now - v12.pdf página 17	Verificado
8	Modificación de archivo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Todas estas técnicas de monitoreo de actividad sospechosa son propias de la solución de sandboxing de Checkpoint. Ver https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/ Ver SandBlast Now - v12.pdf página 17	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

9	Inyección de código Kernel	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Todas estas técnicas de monitoreo de actividad sospechosa son propias de la solución de sandboxing de Checkpoint. Ver https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/ Ver SandBlast Now - v12.pdf página 17	Verificado
10	Detectar intentos de escalamiento de privilegios	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Todas estas técnicas de monitoreo de actividad sospechosa son propias de la solución de sandboxing de Checkpoint. Ver https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/ Ver SandBlast Now - v12.pdf página 17	Verificado
11	Modificaciones del núcleo (cambios en la memoria realizados por el código del kernel, no el hecho de que se cargue un controlador; esto está cubierto por el elemento anterior)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Todas estas técnicas de monitoreo de actividad sospechosa son propias de la solución de sandboxing de Checkpoint. Ver https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/ Ver SandBlast Now - v12.pdf página 17	Verificado
12	Comportamiento del código del kernel (monitoriza la actividad del código no del modo de usuario)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Todas estas técnicas de monitoreo de actividad sospechosa son propias de la solución de sandboxing de Checkpoint. Ver https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			Ver SandBlast Now - v12.pdf página 17	
13	Interacción física directa de la CPU	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Todas estas técnicas de monitoreo de actividad sospechosa son propias de la solución de sandboxing de Checkpoint. Ver https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/ Ver SandBlast Now - v12.pdf página 17	Verificado
14	Detección de derivación UAC (control de acceso de usuario)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Todas estas técnicas de monitoreo de actividad sospechosa son propias de la solución de sandboxing de Checkpoint. Ver https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/ Ver SandBlast Now - v12.pdf página 17	Verificado
J	**Tecnología antievasión:**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	
1	La solución debe tener capacidades antievasión que detecten la ejecución de sandbox	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk167109 • Threat Emulation sandbox enhanced with advanced anti evasion techniques to improve prevention of malware that tries to detect emulation and hide its malicious activities.	Verificado

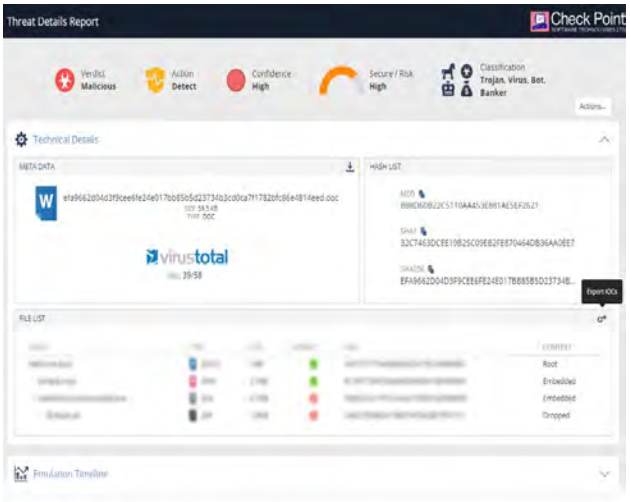
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			https://evasions.checkpoint.com/ Ver SandBlast Now - v12.pdf pagina 15 y 17	
2	La solución debe ser resistente a los casos en los que el código de shell o el malware no se ejecutarían si detectan la existencia de un entorno virtual. (hipervisor propietario)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://www.checkpoint.com/es/quantum/advanced-network-threat-prevention/ https://evasions.checkpoint.com/ Ver SandBlast Now - v12.pdf pagina 15 y 17	Verificado
3	retrasos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://evasions.checkpoint.com/techniques/timing.html Ver SandBlast Now - v12.pdf pagina 15 y 17	Verificado
4	La solución debe ser resistente a las demoras implementadas en el código del shell o en las etapas de malware.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://evasions.checkpoint.com/ Ver SandBlast Now - v12.pdf pagina 15 y 17	Verificado
5	apagado, reinicio	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://evasions.checkpoint.com/ Ver SandBlast Now - v12.pdf pagina 15 y 17	Verificado
6	La solución debe ser resistente a los casos en los que el código de shell o el malware se ejecutan solo al reiniciarse o al	**ENTERADOS, ACEPTAMOS Y**	https://evasions.checkpoint.com/ Ver SandBlast Now - v12.pdf pagina 15 y 17	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	apagarse el punto final.	**CUMPLIMOS**		
7	La interacción del usuario	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**https://evasions.checkpoint.com/** Ver SandBlast Now - v12.pdf pagina 15 y 17	Verificado
8	Emulación humana: la solución debe emular las actividades reales del usuario, como los clics del mouse, las teclas, etc.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://evasions.checkpoint.com/ https://evasions.checkpoint.com/techniques/human-like-behavior.html Ver SandBlast Now - v12.pdf pagina 15 y 17	Verificado
9	Similitud de icono: la solución debería ser capaz de identificar íconos que son similares a los documentos de aplicaciones populares	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver SandBlast Now - v12.pdf pagina 15 y 17	Verificado
10	evasión dentro de archivo flash (swf)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	SANDBLAST NETWORK – SPECIFICATIONS THREAT EMULATION Emulation Environments: • PC: Windows XP or later • Mac: MacOS version 10.14.6 (Mojave) or later File Types: Over 70 file types emulated, including: Microsoft Office documents and templates, EXE, DLL, Archives (ISO, ZIP, 7Z, RAR, etc.), PDF, Flash, Java, scripts and more. Archive Files: • Archived (compressed) files • Password protected archives THREAT EXTRACTION	Verificado
K	**Gestión e informes**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

1	Tras la detección de archivos maliciosos, se debe generar un informe detallado para cada uno de los archivos maliciosos.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
2	El informe detallado debe incluir:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120357**	Verificado
3	video de la emulación	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120357	Verificado
4	líneas de tiempo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120357	Verificado
5	creación / modificaciones de clave de registro,	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120357	Verificado
6	creación de archivos y procesos	**ENTERADOS, ACEPTAMOS Y**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120357	

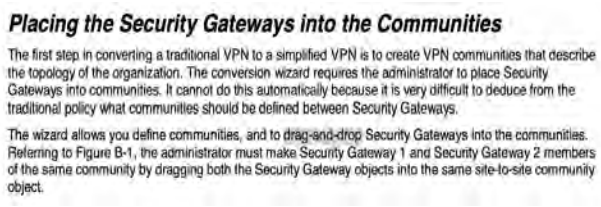
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLIMOS		Verificado
7	Actividad de red detectada.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120357	Verificado
L	**Extracción de amenazas (depuración / aplanamiento de archivos)**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	
1	la solución debería eliminar amenazas y eliminar contenido explotable, incluido contenido activo y objetos incrustados	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://blog.checkpoint.com/2019/10/10/threat-extraction-a-preventive-method-for-document-based-malware/	Verificado
2	la solución debería poder Reconstruir archivos con elementos seguros conocidos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	CP_R81_ThreatPrevention_AdminGuide.pdf página 83	Verificado
3	la solución debe proporcionar la capacidad de convertir archivos reconstruidos a formato PDF	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	CP_R81_ThreatPrevention_AdminGuide.pdf página 83	Verificado
4	la solución debe mantener flexibilidad con opciones para mantener el formato de archivo original y especificar el tipo de contenido que se eliminará	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	CP_R81_ThreatPrevention_AdminGuide.pdf página 83	Verificado
M	**IPsec VPN**	**ENTERADOS, ACEPTAMOS Y**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		
1	Se debe admitir la CA interna y la CA externa de terceros.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver CP_R81_SitetoSiteVPN_AdminGuide.pdf pagina 80	Verificado
2	La solución debe admitir cifrado 3DES y AES-256 para IKE Phase I y II IKEv2 más "Suite-B-GCM-128" y "Suite-B-GCM-256" para Fase II	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver CP_R81_SitetoSiteVPN_AdminGuide.pdf pagina 46, 48, 49 https://sc1.checkpoint.com/documents/R80/CP_R80_SmartDashboard_OLH/html_frameset.htm?topic=documents/R80/CP_R80_SmartDashboard_OLH/gZ-r8TnMA_RLMUqax8xU1A2	Verificado
3	La solución debe admitir al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bits), Grupo 2 (1024 bits), Grupo 5 (1536 bits), Grupo 14 (2048 bits), Grupo 19 y Grupo 20	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver CP_R81_SitetoSiteVPN_AdminGuide.pdf pagina 48	Verificado
4	La solución debe ser compatible con la integridad de los datos con md5, sha1 SHA-256, SHA-384 y AES-XCBC	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver CP_R81_SitetoSiteVPN_AdminGuide.pdf pagina 48	Verificado
5	La solución debe incluir soporte para VPN de sitio a sitio en las siguientes topologías:	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver CP_R81_SitetoSiteVPN_AdminGuide.pdf	Verificado
6	Full Mesh (todos para todos),	**ENTERA DOS, ACEPTA**	Ver CP_R81_SitetoSiteVPN_AdminGuide.pdf pagina 38, 39	

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		MOS Y CUMPLI MOS		Verificado
7	Estrella (oficinas remotas al sitio central)	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver CP_R81_SitetoSiteVPN_AdminGuide.pdf pagina 38, 39	Verificado
8	Hub and Spoke (sitio remoto a través del sitio central a otro sitio remoto)	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver CP_R81_SitetoSiteVPN_AdminGuide.pdf pagina 24	Verificado
9	La solución debe ser compatible con la configuración de VPN con una GUI mediante la adición de objetos de arrastrar y soltar a las comunidades de VPN	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver CP_R75_VPN_AdminGuide.pdf pagina 137  ***Placing the Security Gateways into the Communities*** The first step in converting a traditional VPN to a simplified VPN is to create VPN communities that describe the topology of the organization. The conversion wizard requires the administrator to place Security Gateways into communities. It cannot do this automatically because it is very difficult to deduce from the traditional policy what communities should be defined between Security Gateways. The wizard allows you define communities, and to drag-and-drop Security Gateways into the communities. Referring to Figure B-1, the administrator must make Security Gateway 1 and Security Gateway 2 members of the same community by dragging both the Security Gateway objects into the same site-to-site community object.	Verificado
10	La solución debe admitir VPN SSL sin cliente para el acceso remoto.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver CP_R81_SitetoSiteVPN_AdminGuide.pdf pagina 149, 150, 151, 152-154	Verificado
11	La solución debe ser compatible con VPN L2TP, incluida la compatibilidad con el cliente de iPhone L2TP	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver CP_R81_SitetoSiteVPN_AdminGuide.pdf pagina 114	Verificado
12	La solución debe permitir que el administrador aplique reglas de seguridad para controlar el tráfico dentro de la VPN	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Ver CP_R81_SitetoSiteVPN_AdminGuide.pdf pagina 41	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

13	La solución debe admitir redes privadas virtuales (VPN) basadas en dominio y VPN basadas en rutas que utilicen VTI y protocolos de enrutamiento dinámico.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/VPN-Tunnel-Interfaces.htm https://sc1.checkpoint.com/documents/R76/CP_R76_VPN_AdminGuide/13824.htm “Dynamic routing protocol”	Verificado
14	La solución debe incluir la capacidad de establecer VPN con puertas de enlace con IP públicas dinámicas	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://community.checkpoint.com/t5/General-Topics/VPN-tunnel-with-Dynamic-IP-address/td-p/15116 Dynamically Assigned IP Security Gateways A Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway where the external interface's IP address is assigned dynamic ally by the ISP. Creating VPN tunnels with DAIP Security Gateways are only supported by using certificate authentication. Peer Security Gateways identify internally managed DAIP Security Gateways using the DN of the certificate. Peer Security Gateways iden tify externally managed DAIP Security Gateways and 3rd party DAIP Security Gateways using the Matching Criteria configuration DAIP Security Gateways may initiate a VPN tunnel with non -DAIP Security Gateways. However, since a DAIP Security Gateway's external IP address is always changing, peer Security Gateways cannot know in advance which IP address to use to connect to the DAIP Security Gateway. As a result, a peer Security Gateway cannot initiate a VPN tunnel with a DAIP Security Gateway unless DNS Resolv ing is configured on the DAIP Security Gateway. For more information, see Link Selection (on page 96). If the IP on the DAIP Security Gateway changes during a session, it will renegotiate IKE using the newly assigned IP address. In a star community when VPN routing is configured, DAIP Security Gateways cannot initiate connections from their external IP through the center Security Gateway(s) to other DAIP Security Gateways or through the center to the Internet. In this configuration, connections from the encryption domain of the DAIP are	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

15	La solución debe incluir compresión de IP para VPNs de cliente a sitio y sitio a sitio	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_SitetoSiteVPN_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_SitetoSiteVPN_AdminGuide/13847 *IP Compression* IP compression is a process that reduces the size of the data portion of the TCP/IP packet. Such a reduction can cause significant improvement in performance. IPsec supports the *Flate/Deflate* IP compression algorithm. Deflate is a smart algorithm that adapts the way it compresses data to the actual data itself. Whether to use IP compression is decided during IKE phase II. IP compression is not enabled by default. IP compression is important for Remote Access client users with slow links. Security Gateway encryption makes TCP/IP packets appear "mixed up". This kind of data cannot be compressed and bandwidth is lost as a result. If IP compression is enabled, packets are compressed *before* encryption. This has the effect of recovering the lost bandwidth.	Verificado
N	**Gestión de seguridad**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	
1	Las comunicaciones entre todos los componentes que pertenezcan a la solución total (servidor de administración, gateways), deben establecer comunicaciones seguras y cifradas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Secure-Internal-Communication.htm	Verificado
2	Debe incluir una herramienta de búsqueda, que permita fácilmente filtrar objetos de red. Debe también incluir la opción de buscar objetos duplicados (con la misma IP) y	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **CP_R81_Quantum_SecurityManagement_AdminGuide.pdf páginas 37,38,39**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	objetos no usados (en una regla o política) y una lista de las reglas en que un objeto especifico es usado			
3	Debe poderse realizar un cambio automático de logs, basados en programaciones de tiempo o del tamaño del archivo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 519 - 522	Verificado
4	La solución debe tener la capacidad de hacer auditorias de las acciones de cada administrador que acceda a la plataforma	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=documents/R80/CP_R80_LoggingAndMonitoring/120828 Audit Log A record of an action that is done by an Administrator. See also Log	Verificado
5	La solución debe permitir realizar un completa auditoria, seguimiento en los cambios y evolución de las políticas de seguridad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 178	Verificado
6	La solución debe tener la capacidad de forma nativa en tiempo real, de dar información sobre el estado de los dispositivos administrados (conectividad, nivel cpu, tráfico de red) e ilustrar de forma gráfica al menos eventos como la	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R80.10_Gaia_AdminGuide.pdf pagina 19, 20 Ver DS_Monitoring.pdf pagina 2,3 CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 156	Verificado

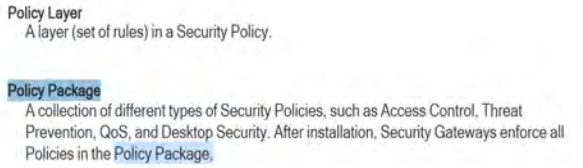
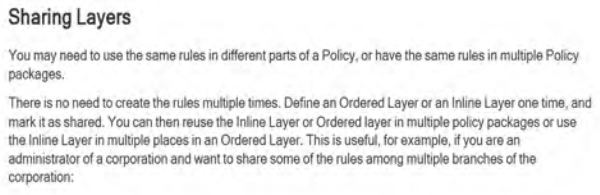
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	conexión de usuarios remotos via vpn, estado de los túneles IPSEC y trafico más común sobre las interfaces (monitor)			
7	Debe poder restringirse que direcciones IP (direcciones individuales, rangos, hostnames) pueden tener control sobre la consola de administración	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Gaia_AdminGuide.pdf página 292	Verificado
8	Capacidad de funcionar en un esquema de alta disponibilidad, para evitar que exista un solo momento de pérdida de funcionalidad de administración.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk54160	Verificado
9	La autenticación de administradores al sistema debe poder ser por lo menos mediante contraseña (password), certificados digitales y sistemas RADIUS	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/124265	Verificado
10	Debe permitir la creación de filtros basados en cualquiera de las características del evento, tales como IP de origen y destino, servicio, tipo de evento, severidad del evento, nombre del ataque, país de origen o destino, etc. El administrador debe	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 27, 90, 100,101,102 Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 178	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	poder asignar estos filtros a diferentes líneas en un gráfico que sean actualizadas en intervalos regulares mostrando todos los eventos que concuerdan con ese filtro. Permitiendo que el operador se focalice en los eventos más importantes.			
11	La solución debe ser capaz de segmentar la base de reglas en una estructura de subpolíticas en la que solo el tráfico relevante se está reenviando al segmento relevante	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf páginas 173, 174,175,176, 180,204,205	Verificado
12	La solución debe ser capaz de segmentar la base de reglas a favor de la delegación de funciones en las que los cambios en un segmento no afectarán a otros segmentos.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 180, 196	Verificado
13	La solución debe poder segmentar la base de reglas en una estructura en capas	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 180, 204,205	Verificado
14	La solución debe poder segmentar la base de reglas para permitir la flexibilidad de la estructura para alinearse con redes dinámicas	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 180, 204,205	Verificado

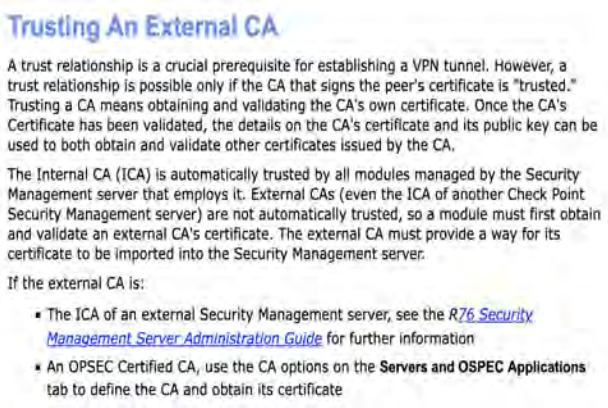
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

15	La solución debe poder reutilizar el segmento de la base de reglas (por ejemplo, usar el mismo segmento de reglas en diferentes paquetes de políticas)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 28 “Policy Package”  Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 212 	Verificado
16	La solución debe tener la granularidad de los administradores que trabajan en paralelo en la misma política sin interferir entre ellos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 212	Verificado
17	La solución debe integrar registros, registros de auditoría en una consola para tener contexto mientras se trabaja	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 27, 90, 100,101,102	Verificado

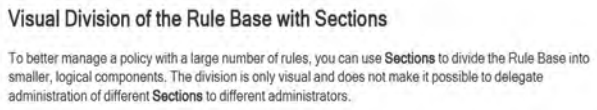
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	en la política de seguridad		Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 178	
18	La solución debe ser capaz de instalar protecciones relacionadas con amenazas y acceder a reglas relacionadas por separado para permitir su administración por equipos separados.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 212  Administrators for Access Control Layers You can create administrator accounts dedicated to the role of Access Control, with their own installation and SmartConsole Read/Write permissions. You can also delegate ownership of different Layers to different administrators. See *"Configuring Permissions for Access Control Layers" on page 116.*	Verificado
19	La aplicación de administración de seguridad debe admitir cuentas de administrador basadas en roles. Por ejemplo, funciones para la administración de políticas de firewall solamente o rol para visualización de registros solamente	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 113, 115  Assigning Permission Profiles to Administrators A permission profile is a predefined set of Security Management Server and SmartConsole administrative permissions that you can assign to administrators. You can assign a permission profile to more than one administrator. Only Security Management Server administrators with the *Manage Administrators* permission in the profile can create and manage permission profiles. Configuring Customized Permissions Configure administrator permissions for Gateways, **Access Control**, **Threat Prevention**, **Others**, **Monitoring and Logging**, **Events and Reports**, **Management**. For each resource, define if administrators that are configured with this profile can configure the feature or only see it.	Verificado
20	La solución debe incluir un canal de comunicaciones seguro cifrado basado en certificado entre todos los componentes distribuidos por el proveedor que pertenecen a un único dominio de gestión	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Secure-Internal-Communication.htm	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

21	La solución debe incluir una CA x.509 interna (Autoridad de certificación) que pueda generar certificados para las puertas de enlace y los usuarios para permitir una autenticación fácil en VPN.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 347	Verificado
22	La solución debe incluir la capacidad de utilizar CA externas, que sea compatible con las normas PKCS # 12, CAPI o Entrust	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 353 https://sc1.checkpoint.com/documents/R76/CP_R76_VPN_AdminGuide/13914.htm  **Trusting An External CA** A trust relationship is a crucial prerequisite for establishing a VPN tunnel. However, a trust relationship is possible only if the CA that signs the peer's certificate is "trusted." Trusting a CA means obtaining and validating the CA's own certificate. Once the CA's Certificate has been validated, the details on the CA's certificate and its public key can be used to both obtain and validate other certificates issued by the CA. The Internal CA (ICA) is automatically trusted by all modules managed by the Security Management server that employs it. External CAs (even the ICA of another Check Point Security Management server) are not automatically trusted, so a module must first obtain and validate an external CA's certificate. The external CA must provide a way for its certificate to be imported into the Security Management server. If the external CA is: ▪ The ICA of an external Security Management server, see the *R76 Security Management Server Administration Guide* for further information ▪ An OPSEC Certified CA, use the CA options on the **Servers and OSPEC Applications** tab to define the CA and obtain its certificate	Verificado
23	La administración debe proporcionar un contador de visitas a las normas de seguridad en la política de seguridad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 229 “Hits”	Verificado
24	La solución debe incluir una opción de búsqueda para poder consultar fácilmente qué objeto de red contiene una dirección IP	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 37, 38 “Search”	Verificado

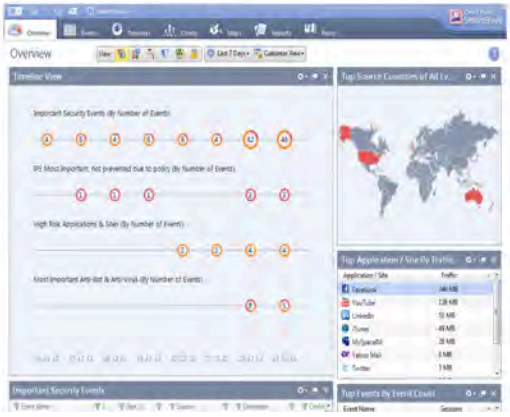
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	específica o parte de ella			
25	La solución debe incluir la opción de segmentar la base de reglas usando etiquetas o títulos de secciones para organizar mejor la política.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 213  Visual Division of the Rule Base with Sections To better manage a policy with a large number of rules, you can use **Sections** to divide the Rule Base into smaller, logical components. The division is only visual and does not make it possible to delegate administration of different **Sections** to different administrators.	Verificado
26	La solución debe proporcionar la opción de guardar toda la política o parte específica de la política	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 173 “policy package”	Verificado
27	La solución debe tener un mecanismo de verificación de la política de seguridad antes de la instalación de la política	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/119225 “Installing a Policy Package”, “Validation errors”	Verificado
28	La solución debe tener un mecanismo de control de revisión de la política de seguridad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 178 “Policy Installation History”	Verificado
29	La solución debe incluir la capacidad de distribuir de forma centralizada y aplicar nuevas versiones de software de puerta de enlace	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Gaia_AdminGuide.pdf pagina 455	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

30	La solución debe incluir una herramienta para administrar centralmente las licencias de todas las puertas de enlace controladas por la estación de administración	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 132	Verificado
31	La solución debe tener las capacidades para la administración multidominio y respaldar el concepto de política de seguridad global en todos los dominios	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://www.checkpoint.com/quantum/multi-domain-security-management/	Verificado
32	Debe mostrar la distribución de eventos por países en un mapa.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 77 https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmin/92712.htm	

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			Monitoring Important Events with SmartEvent The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartEvent consolidates and shows all security events that are generated by these Software Blades: • Firewall • Identity Awareness, and URL Filtering • IPS • Application Control • Anti-Bot, Threat Emulation, and Anti-Virus • DLP Administrators can quickly identify very important security events and do the necessary actions to prevent more attacks. 	Verificado
33	Debe permitir agrupar los eventos en base a cualquier característica de los mismos, pudiendo agrupar en varios niveles.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 27, 90, 100,101,102 Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 178	Verificado
34	Debe permitir realizar búsquedas dentro del listado de eventos.	**ENTERADOS, ACEPTAMOS Y**	Ver	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLIMOS	CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 24, 27, 90, 100,101,102 Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 178	
35	La GUI de administración debe tener la capacidad de excluir fácilmente la dirección IP de la definición de firma IPS.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92707.htm **Adding Network Exceptions** You can configure exceptions for a protection with the **Prevent** action, so that it does not identify the specified traffic. These are some situations where it is helpful to use exceptions: ▪ Traffic that is legitimate for some machines or services can match the protection criteria for malware. ▪ A server that does not comply with RFC standards. ***Adding an IPS Exception*** To add a new exception: 1. In the **IPS** tab, select **Network Exceptions**. 2. Click **New**. The **Add/Edit Exception Rule** window opens 3. From **Profile**, select a profile or **Any**. 4. From **Protection**, select the excluded protection(s). ▪ **Single protection** - Click **Select** and then select the protection. ▪ **All supported protections** - Only protections that support the Network Exceptions feature are excluded. 5. Define the **Source** and **Destination**, and **Service** for the excluded protection. ▪ To use a SmartDashboard object, click **Manage** and then select the object.	Verificado
36	El Visor de registro debe tener la capacidad de excluir fácilmente la dirección IP de los registros de IPS cuando se detecta como falso positivo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R76/CP_R76_IPS_AdminGuide/12766.htm 4. In the **Scope** area, select the protection that will be affected by this exception: ▪ **All supported protections**: IPS will exclude traffic from inspection based on s destination, or service; this effectively turns off IPS inspection for the traffi matches the exceptions. Protections that do not support the Network Excep will not be affected.	

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

				Verificado
37	La GUI de administración debe tener la capacidad de acceder fácilmente a la definición de firmas IPS a partir de los registros de IPS	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

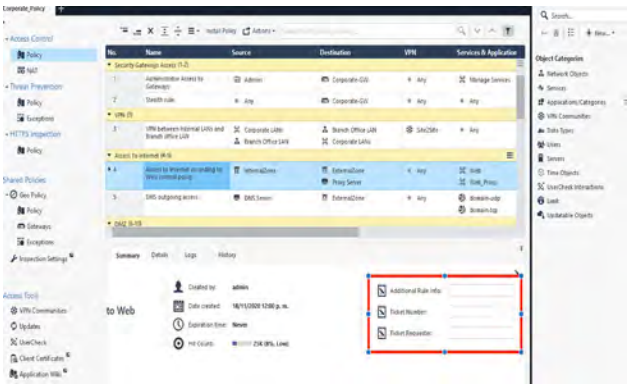
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

38	Debe soportar agendar reportes para que se ejecuten automáticamente para extraer información en periodos regulares de tiempo (diarios, semanales y mensuales). También debe permitir al administrador la fecha y horario en que empezará a generar el reporte agendado.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Scheduling-view-or-report.htm	Verificado
39	El Visor de registro debe tener la capacidad de ver todos los registros de seguridad (fw, IPS, urlf ...) en un panel de visualización (útil cuando se soluciona un problema de conectividad para una dirección IP)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 27, 90, 100,101,102 Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 178	Verificado
40	La herramienta de reportes debe soportar al menos 25 filtros (ej. Origen, destino, nombre del ataque, número de regla) que permita personalizar los reportes predefinidos a las necesidades del administrador (ej. Actividades web de un usuario especifico)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R80/CP_SmartEvent_R80_Views_and_Reports_Tutorial_web/EN/html_frameset.htm?topic=documents/R80/CP_SmartEvent_R80_Views_and_Reports_Tutorial_web/EN/131064	Verificado
41	El Visor de registro debe tener la capacidad en el visor de registro de crear un filtro utilizando los objetos predefinidos (hosts, red, grupos, usuarios ...)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R80/CP_SmartEvent_R80_Views_and_Reports_Tutorial_web/EN/html_frameset.htm?topic=documents/R80/CP_SmartEvent_R80_Views_and_Reports_Tutorial_web/EN/131064	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

42	El Visor de registro debe tener la capacidad en el visor de registro para crear múltiples "filtros guardados" personalizados para usar en un momento posterior.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R80/CP_SmartEvent_R80_Views_and_Reports_Tutorial_web/EN/html_frameset.htm?topic=documents/R80/CP_SmartEvent_R80_Views_and_Reports_Tutorial_web/EN/131064 	Verificado
43	La solución de administración de políticas debe proporcionar registros de reglas similares para el usuario a medida que crea o modifica reglas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_LoggingAndMonitoring_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_LoggingAndMonitoring_AdminGuide/131914	Verificado
44	La GUI de la solución debe proporcionar una navegación fácil entre cientos de políticas, cada una con hasta 1 millón de reglas. Se deben proporcionar saltos entre subpolíticas y títulos de sección, así como una búsqueda exhaustiva.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 37, 38, “Search”, 205 “Inline Layers”	Verificado
45	La administración de políticas debe proporcionar la búsqueda de reglas por paquetes, incluso sin tener registros de ese paquete en el	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 37, 38, “Search”, 205 “Inline Layers”	Verificado

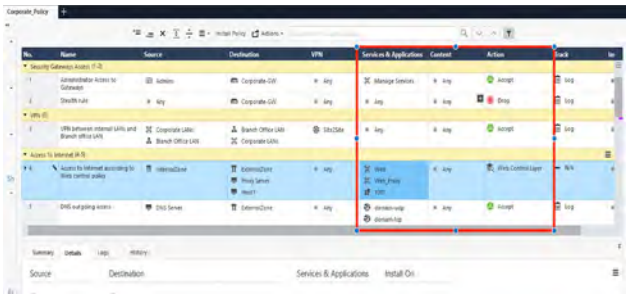
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	sistema. La búsqueda debe estar integrada en el mismo panel que la configuración de la política y devolver todos los resultados en pocos segundos.			
46	La solución de administración de seguridad debe proporcionar la búsqueda de todas las referencias a cualquier objeto de red dado en todas sus políticas y configuraciones (donde se usa).	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 37, 38, “Search”,	Verificado
47	La solución debe proporcionar administración integrada de tickets. Se debe asociar automáticamente a una sesión un conjunto de cambios en la política de seguridad para lograr la responsabilidad y la documentación adecuadas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
48	La administración de seguridad debe proporcionar un conjunto de mejores prácticas de seguridad incorporadas que proporcionan puntaje automático para varias regulaciones de seguridad.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver compliance-datasheet.pdf https://www.checkpoint.com/quantum/security-compliance/	Verificado

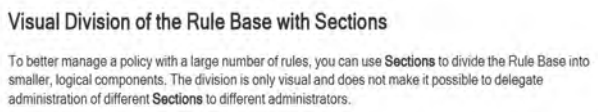
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

49	La administración de seguridad debe tener la opción de alertar a los usuarios sobre una posible configuración incorrecta, al tiempo que les proporciona una forma de agregar excepciones a estas posibles configuraciones erróneas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver compliance-datasheet.pdf https://www.checkpoint.com/quantum/security-compliance/	Verificado
50	El usuario debe proporcionar detalles de NAT para un objeto de red en el alcance del objeto de red. Las reglas NAT inferidas se deben agregar automáticamente a la política NAT.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 240	Verificado
51	El usuario debería ser capaz de tratar sin problemas los objetos IPV4, IPV6 y de red dinámica en la misma política.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución es totalmente compatible con IPV6, se pueden crear objetos IPV4 e IPV6 y mezclarlos en la misma política de seguridad. 	Verificado
52	La pasarela de seguridad debe inspeccionar el tráfico de la red, el contexto de la aplicación y los datos y el contenido dentro de una regla.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución permite inspeccionar el tráfico de la red, el contexto de la aplicación y los datos y el contenido dentro de una regla.	

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

				Verificado
53	El sistema IPS debe proporcionar acciones automáticas en Protecciones IPS basadas en las definiciones del usuario de sus activos críticos.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_ThreatPrevention_AdminGuide.pdf página 170	Verificado
54	El sistema IPS debe proporcionar perfiles inteligentes en tres niveles en el eje de seguridad frente al rendimiento. El usuario puede optar por habilitar protecciones granulares o, en su lugar, elegir uno de los perfiles inteligentes.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_ThreatPrevention_AdminGuide.pdf página 167 – 174 https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Topics-TPG/Configuring-IPS-Profile-Settings.htm 	Verificado
55	Al crear o editar políticas de seguridad se debe poder forzar el uso de una descripción, tag o comentario de auditoria. Esto con el fin de garantizar	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 213	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	buenas prácticas de documentación y organización y auditoría.			
56	La solución de permitir modificar e instalar políticas al mismo tiempo por diferentes administradores de la solución.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Concurrent-Install-Policy.htm	Verificado
57	La solución a ofertar deber permitir hacer un check de la configuración realizada antes de hacer un instalación de políticas a fin de poder revisar cualquier mala configuración o solapamiento de políticas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/119225 "Installing a Policy Package", "Validation errors"	Verificado
58	La solución debe permitir configurar diferenciar roles a los usuarios administradores a fin de poder limitar su funciones y no tener un control global de la plataforma.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 113, 115 	Verificado

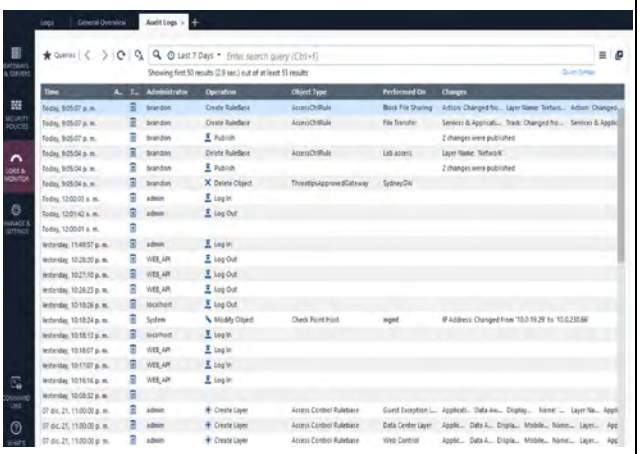
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

O	**Actualizaciones de prevención de amenazas**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	
1	El proveedor debe proporcionar los detalles de su mecanismo de actualización de prevención de amenazas y su capacidad para manejar ataques de día cero en todas las aplicaciones de prevención de amenazas de próxima generación, incluyendo IPS, Control de aplicaciones, filtrado de URL, Anti-Bot y Anti-Virus.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_ThreatPrevention_AdminGuide.pdf página 250	Verificado
2	El proveedor debe proporcionar detalles sobre la reclasificación de URL, en las circunstancias en que se ha incluido un sitio web y, posiblemente, la distribución de malware	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk69200 https://urlcat.checkpoint.com/urlcat/main.htm	Verificado
3	El proveedor debe tener la capacidad de proporcionar manejo de incidentes	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Softsecurity cuenta con una mesa de ayuda e ingenieros certificados en la solución propuesta, de tal manera que Softsecurity cuenta con la capacidad de proporcionar el manejo de incidentes.	Verificado
P	**Registro y Monitoreo**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	

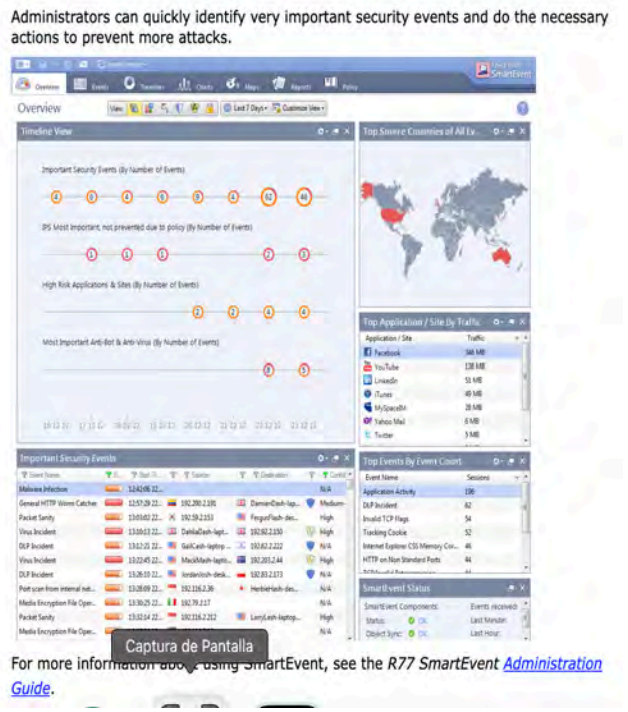
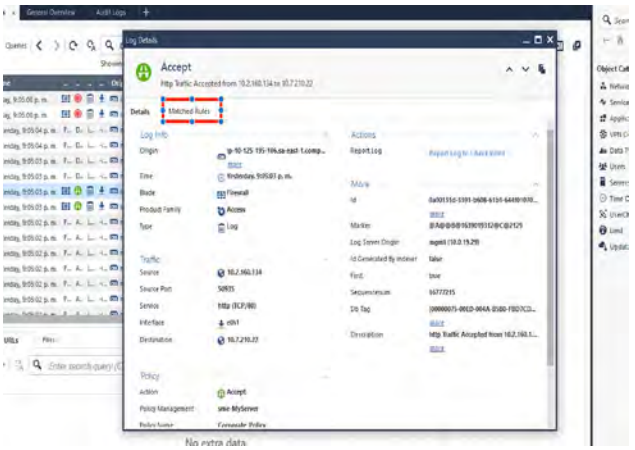
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	El registro central debe ser parte del sistema de gestión.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 24	Verificado
1	El visor de registros debe tener una capacidad de búsqueda indexada	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 35	Verificado
2	La solución debe tener la capacidad de registrar todas las aplicaciones de seguridad integradas en la puerta de enlace e incluir IPS, Control de aplicaciones, Filtrado de URL, Antivirus, Anti-Bot, Anti-Spam, Identidad de usuario, Prevención de pérdida de datos, Acceso móvil	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver smartevent-datasheet.pdf CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 24,25	Verificado
3	La solución debe incluir un mecanismo automático de captura de paquetes para eventos IPS para proporcionar un mejor análisis forense	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_LoggingAndMonitoring_AdminGuide/Topics-LMG/Packet-Capture.htm	Verificado
4	La solución debe proporcionar registros diferentes para la actividad habitual del usuario y los registros relacionados con la gestión.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_LoggingAndMonitoring_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_LoggingAndMonitoring_AdminGuide/131914 https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmin/92712.htm	Verificado

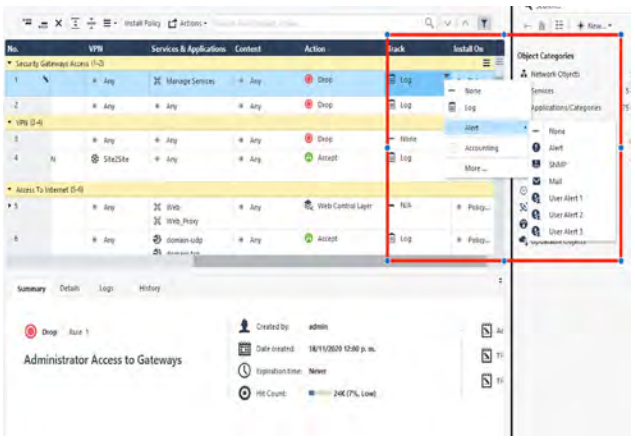
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			Monitoring Important Events with SmartEvent The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartEvent consolidates and shows all security events that are generated by these Software Blades: ▪ Firewall ▪ Identity Awareness, and URL Filtering ▪ IPS ▪ Application Control ▪ Anti-Bot, Threat Emulation, and Anti-Virus ▪ DLP Administrators can quickly identify very important security events and do the necessary actions to prevent more attacks. Log de gestión 	
5	Debe proveer un reportador en tiempo real basado en una línea de tiempo, para reportes predefinidos o a la medida, permitiendo al administrador realizar	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmin/92712.htm	Verificado

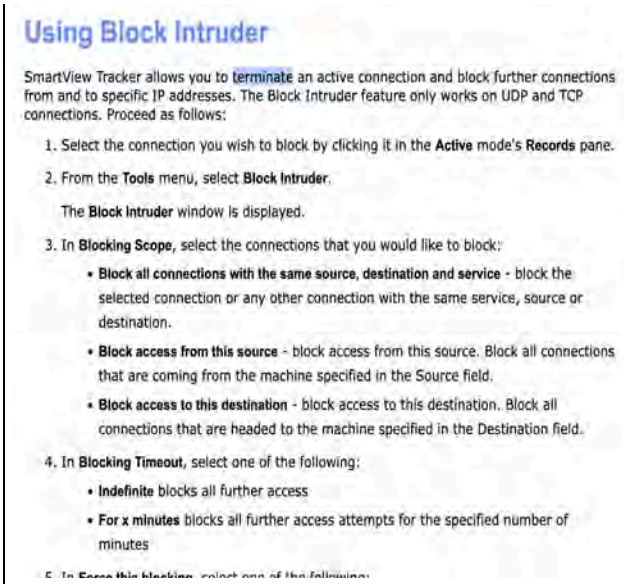
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	análisis de contenido en tiempo real.			
6	La solución debe poder pasar del registro de registro de seguridad a la regla de política con un clic del mouse.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

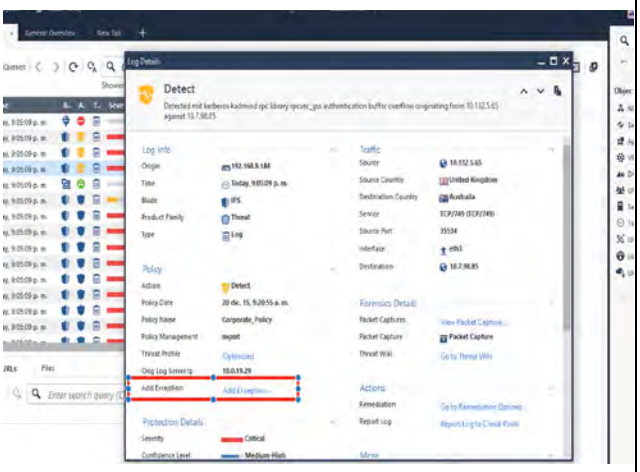
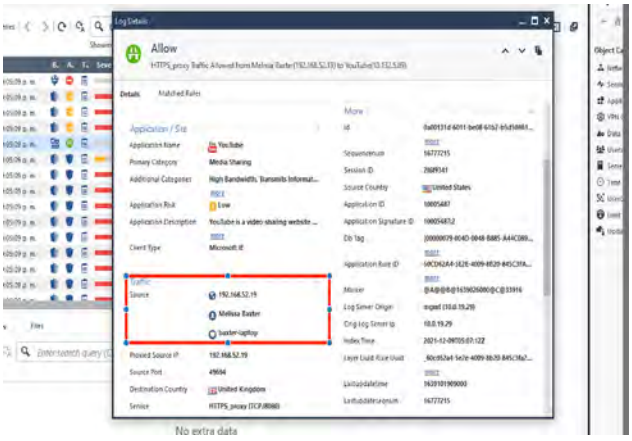
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

7	Para cada regla de coincidencia o tipo de evento, la solución debe proporcionar al menos las siguientes opciones de eventos: registro, alerta, captura de SNMP, correo electrónico y ejecutar una secuencia de comandos definida por el usuario.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
8	Los registros deben tener un canal seguro para transferir el registro para evitar el espionaje, la solución debe ser autenticada y encriptada	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Secure-Internal-Communication.htm	Verificado
9	La solución debe incluir la opción de bloquear dinámicamente una conexión activa desde la interfaz gráfica de registro sin la necesidad de modificar la base de reglas	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R76/CP_R76_SmartView_Tracker_AdminGuide/89751.htm	Verificado

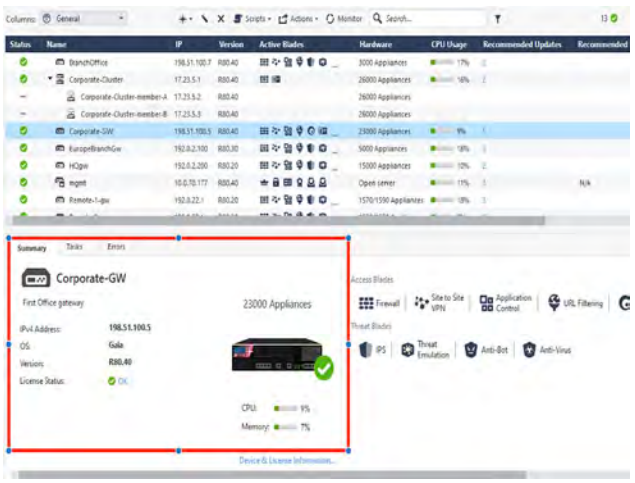
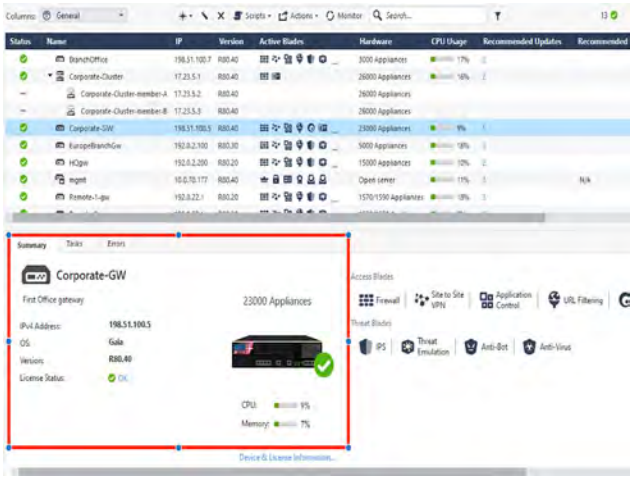
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

				
10	La solución debe ser compatible con la exportación de registros en formato de base de datos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 213	Verificado
11	La solución debe ser compatible con el cambio automático del archivo de registro, en función de un tiempo programado o tamaño de archivo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 533 “fw logswitch” https://sc1.checkpoint.com/documents/R77/CP_R77_SmartViewTracker_AdminGuide/89751.htm	Verificado

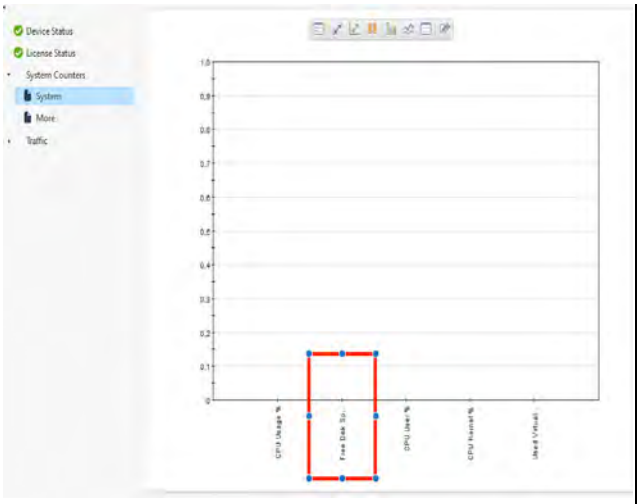
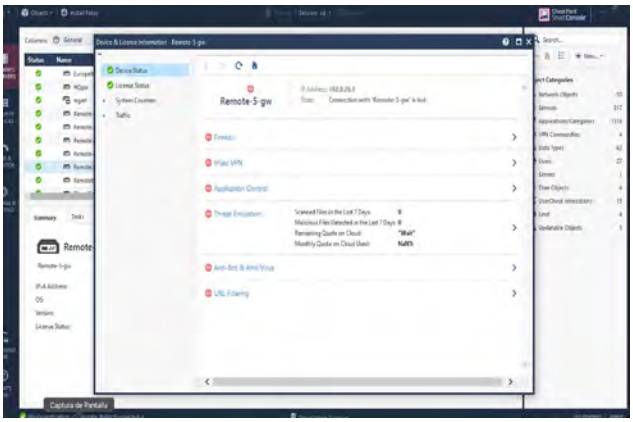
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

12	La solución debe admitir la adición de excepciones a la aplicación de IPS del registro de registro	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
13	La solución debe poder asociar un nombre de usuario y nombre de máquina a cada registro de registro	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

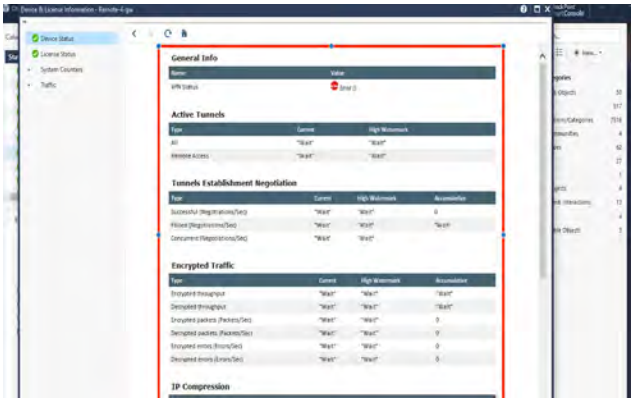
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

14	La solución debe incluir una interfaz gráfica de monitoreo que proporcione una manera fácil de monitorear el estado de las puertas de enlace	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
15	La solución debe proporcionar la siguiente información del sistema para cada puerta de enlace: sistema operativo, uso de la CPU, uso de la memoria, todas las particiones del disco y % del espacio libre en el disco duro.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

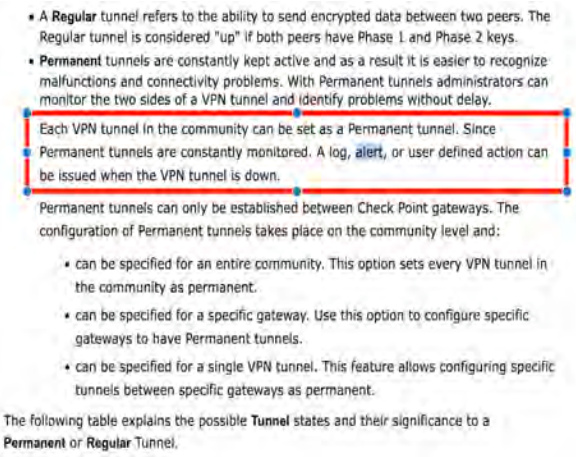
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

				
16	La solución debe proporcionar el estado de cada componente de la puerta de enlace (es decir, firewall, vpn, cluster, antivirus, etc.)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

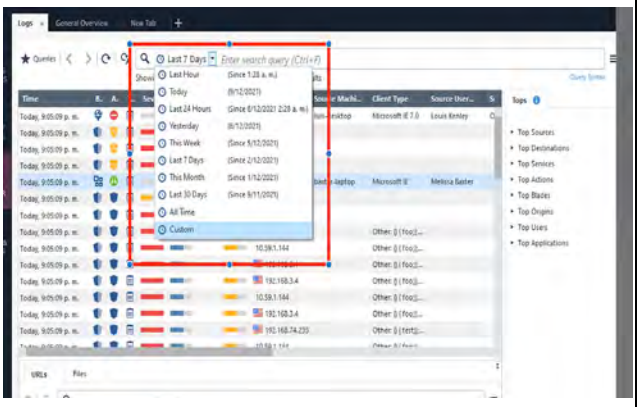
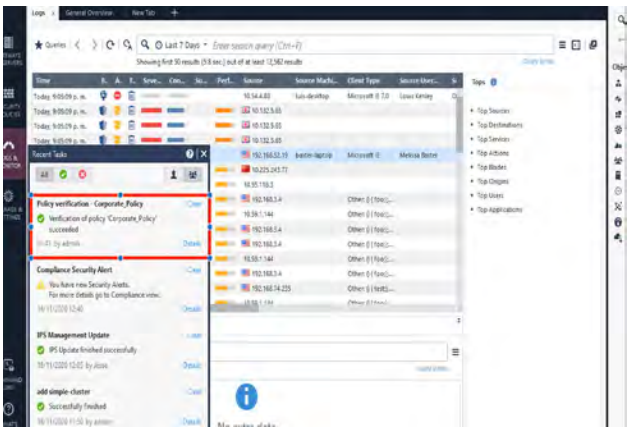
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

17	La solución debe incluir el estado de todos los túneles VPN, sitio a sitio y cliente a sitio	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
18	La solución debe incluir una configuración de umbral personalizable para tomar medidas cuando se alcanza un determinado umbral en una puerta de enlace. Las acciones deben incluir: Registrar, alertar, enviar una trampa SNMP, enviar un correo electrónico y ejecutar una alerta definida por el usuario	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_LoggingAndMonitoring_AdminGuide/Topics-LMG/System-alerts-and-thresholds.htm	Verificado
19	La solución debe incluir gráficos pre configurados para monitorear la evolución en el tiempo del tráfico y los contadores del sistema: reglas de seguridad superiores, usuarios P2P principales, túneles vpn, tráfico de red y otra información útil. La solución debe proporcionar la opción de generar nuevos gráficos personalizados con	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R76/CP_R76_SmartReporter_AdminGuide/5834.htm#o5976 https://sc1.checkpoint.com/documents/R76/CP_R76_SmartEventIntro_AdminGuide/84386.htm	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	diferentes tipos de gráficos			
20	Solución debe incluir la opción de grabar vistas de tráfico y del sistema en un archivo para su posterior visualización en cualquier momento	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R80/CP_SmartEvent_R80_Views_and_Reports_Tutorial_web/EN/html_frameset.htm?topic=documents/R80/CP_SmartEvent_R80_Views_and_Reports_Tutorial_web/EN/131059 ver CP_SmartEvent_R80_Views_and_Reports_Tutorial.pdf	Verificado
21	Solución debe ser capaz de reconocer fallos de funcionamiento y problemas de conectividad, entre dos puntos conectados a través de una VPN, y registrar y alerta cuando el túnel VPN está abajo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R76/CP_R76_SmartViewMonitor_AdminGuide/17672.htm  • A **Regular** tunnel refers to the ability to send encrypted data between two peers. The Regular tunnel is considered "up" if both peers have Phase 1 and Phase 2 keys. • **Permanent** tunnels are constantly kept active and as a result it is easier to recognize malfunctions and connectivity problems. With Permanent tunnels administrators can monitor the two sides of a VPN tunnel and identify problems without delay. Each VPN tunnel in the community can be set as a Permanent tunnel. Since Permanent tunnels are constantly monitored. A log, alert, or user defined action can be issued when the VPN tunnel is down. Permanent tunnels can only be established between Check Point gateways. The configuration of Permanent tunnels takes place on the community level and: • can be specified for an entire community. This option sets every VPN tunnel in the community as permanent. • can be specified for a specific gateway. Use this option to configure specific gateways to have Permanent tunnels. • can be specified for a single VPN tunnel. This feature allows configuring specific tunnels between specific gateways as permanent. The following table explains the possible **Tunnel** states and their significance to a **Permanent** or **Regular** Tunnel.	Verificado
22	Los reportes deben incluir una explicación acerca de las políticas que fueron violadas y que parte del contenido	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_SmartEvent_R80_Views_and_Reports_Tutorial.pdf	Verificado

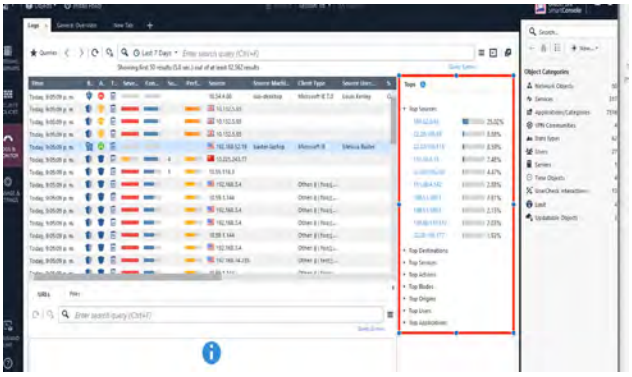
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	causó dicha violación.		https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120256	
23	Los reportes debe mostrar los usuarios (cuando exista una tecnología de AD)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 92 2. Right-click the **User** column and drill down to see the user activity or create a filter for this user in your current view.	Verificado
24	Con el propósito de mejorar la administración, debe ser posible definir un número máximo de alertas para ser mostradas en la GUI, además poder definir un periodo de tiempo máximo para mostrar dichas alertas, por ejemplo mostrar solo las alertas generadas hace una hora.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
25	La solución debe contar con un mecanismo de revisión de políticas, previo a la instalación de las mismas, que ayude a buscar y corregir errores.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

26	El Servidor de administración, debe tener la opción de incorporar una base de datos, de mejores prácticas de seguridad, que provean una calificación, cuando se evalúen temas regulatorios/normativos (ej. ISO27000, NIST)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver compliance-datasheet.pdf página 4	Verificado
27	La solución debe prevenir/ alertar al usuario administrador, cuando trate de realizar cambios que empeoren el alineamiento de la entidad frente a normativas/regulaciones de interés (ej. ISO 27000, NIST)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120256	Verificado
28	El sistema de reportes debe proveer información consolidada sobre al menos:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_LoggingAndMonitoring_AdminGuide.pdf 98,156, 160, 178, https://sc1.checkpoint.com/documents/R76/CP_R76_SmartReporter_AdminGuide/5834.htm	Verificado
	i. Top de eventos por origen			Verificado
	ii. Top de eventos por destino			Verificado
	iii. Eventos por fecha.			Verificado
	iv. Eventos por semana.			Verificado
	v. Top de eventos por producto			Verificado
	vi. Top de eventos por servicios.			Verificado
	vii. Severidad			Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	viii. Producto		Content Inspection Reports Standard Reports ▪ URL Filtering – IMPORTANT: Information in this report is sensitive and must only be provided to users on a need-to-know basis. This report analyzes URL filtering activity by user, category, source and more. Specific sections include: • The top categories of web sites visited • Top web sites visited • Breakdown of blocked lists to URLs • Categories of web sites visited by date and day of week 	Verificado
Q	**Correlación de eventos y presentación de informes**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	
1	Solución debe incluir una herramienta para correlacionar eventos de todas las funciones de puerta de enlace y dispositivos de otros fabricantes	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver smartevent-datasheet.pdf página 3	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

2	La solución debe permitir la creación de filtros basados en cualquier característica del evento como aplicación de seguridad, IP de origen y destino, servicio, tipo de evento, nombre del evento ataque de la gravedad, país de origen y de destino, etc.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 27, 90, 100,101,102 Ver CP_R81_Quantum_SecurityManagement_AdminGuide.pdf página 178	Verificado
3	La aplicación debe tener un mecanismo para asignar estos filtros para diferentes líneas de los gráficos que se actualizan en intervalos regulares que muestran todos los eventos que coincide con el filtro. Permitiendo que el operador se concentre en los eventos más importantes	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 86	Verificado

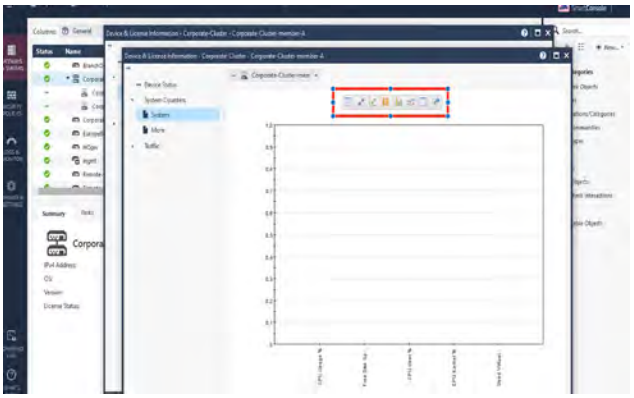
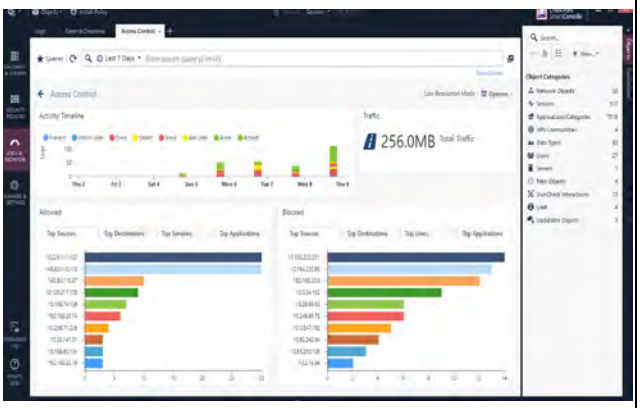
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

4	La aplicación de correlación de eventos debe suministrar una visión gráfica de los eventos en función del tiempo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Administrators can quickly identify very important security events and do the necessary actions to prevent more attacks.  For more information about using SmartEvent, see the *R77 SmartEvent* Administration Guide.	Verificado

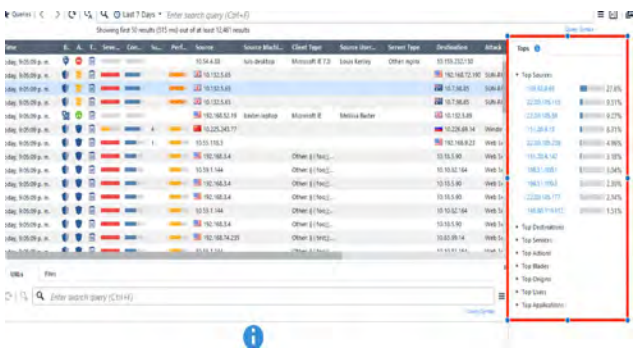
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

5	Solución debe mostrar la distribución de eventos por país en un mapa	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Administrators can quickly identify very important security events and do the necessary actions to prevent more attacks.  For more information about using SmartEvent, see the *R77 SmartEvent* Administration Guide.	Verificado
6	La solución debe permitir al administrador de eventos de grupo basada en cualquiera de sus características, incluyendo muchos niveles de anidamiento y exportar a PDF	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_LoggingAndMonitoring_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_LoggingAndMonitoring_AdminGuide/188029  https://www.checkpoint.com/quantum/event-management/	Verificado

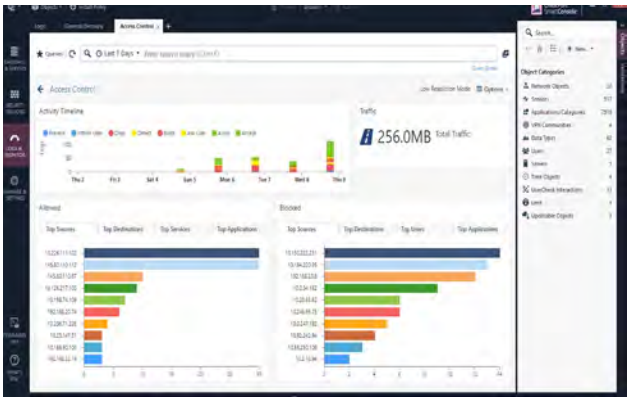
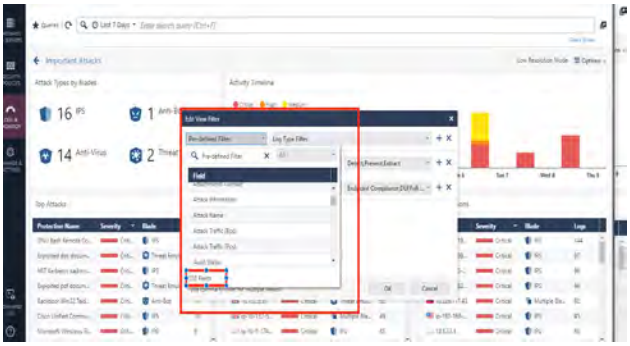
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

7	Solución debe incluir la opción de buscar dentro de la lista de eventos, profundizar en los detalles de la investigación y la medicina forense.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 111	Verificado
8	Es la lista de eventos vista solución debe incluir la opción de generar automáticamente pequeños gráficos o tablas con el evento, el origen y la distribución de destino	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	 	Verificado
9	Solución debe detectar ataques de Denegación de Servicio que correlacionan	**ENTERADOS, ACEPTAMOS Y**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk112241	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	eventos de todas las fuentes	**CUMPLIMOS**	https://www.checkpoint.com/cyber-hub/network-security/what-is-ips/	
10	Solución debe detectar un inicio de sesión de administrador en horas irregulares	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Working-Hours.htm	Verificado
11	Solución debe detectar ataques de adivinanzas de credenciales	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://www.checkpoint.com/defense/advisories/public/2020/cpai-2020-0078.html	Verificado
12	Solución debe informar sobre todas las instalaciones de la política de seguridad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk38929	Verificado
13	Solución debe incluir predefinido por hora, diaria, semanal y mensuales. Incluyendo al menos Top eventos, mejores fuentes, Principales destinos, mejores servicios, mejores fuentes y sus principales eventos, Principales destinos y sus principales eventos y mejores servicios y sus principales eventos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

				
14	La herramienta de informes debe ser compatible con al menos 25 filtros que permiten personalizar un informe predefinido para estar más cerca de las necesidades del administrador	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 80 	Verificado
15	Solución debe ser compatible con la programación de informes automáticos para la información que necesitan para extraer de manera regular (diaria, semanal y mensual). Solución también debe permitir al administrador definir la fecha y hora en que comienza sistema de información para	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R76/CP_R76_SmartReporter_AdminGuide/5867.htm **Report Generation Scheduling** Schedule report generation when there is less traffic and fewer logs are being generated, so that the log consolidator will consume less resources. Schedule reports during the night and on the weekends.	Verificado

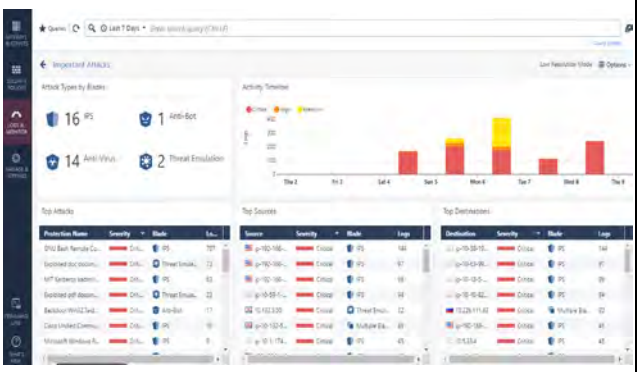
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	generar el informe programado		**Scheduling a Report** To schedule report creation: 1. In the **Reports** view, select **Definitions**. 2. In the **Standard** tab, select **Firewall Blade -> Security > Blocked Connections**. 3. On the **Schedule** tab, click the **Add** button to create a new schedule or the **Edit** button to revise an existing schedule. • **Frequency** - In this area select how often you would like the report to be generated. • **Generate On** - With this option select the date on which SmartReporter should begin to generate the report. • **Schedule time** - With this option select the time at which SmartReporter should begin to generate the report. • **Schedule activation period** - This section is available once you decide the report should be generated more than one. In this area select the date on which SmartReporter should begin to generate the report and the date on which SmartReporter should stop generating the report (if at all).	
16	Solución debe ser compatible con los siguientes formatos: informes HTML, CSV y MHT	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R76/CP_R76_SmartEventIntro_AdminGuide/84386.htm **To configure email settings for each defined report:** 1. Select a report in the **Reports** tree and click **Manage**. 2. Go to the **Email Settings** pane. 3. Select the **Send By Email** option (cleared by default). You must select this option to automatically send reports by email. 4. Select the **Custom** option. 5. Enter recipient email addresses in the **To** and **Cc** fields. You can enter many email addresses in each field, separated by a semicolon. 6. Select the **Report Format**: • **HTML** • **PDF** **MHT** - MIME HTML archive format	Verificado
17	Solución debe ser compatible con la distribución automática de informes por correo electrónico, subir a un servidor FTP / Web y un script de distribución de informes personalizados externa	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://sc1.checkpoint.com/documents/R76/CP_R76_SmartEventIntro_AdminGuide/84386.htm	

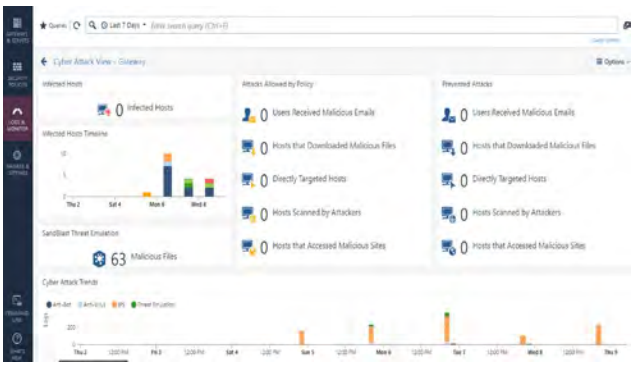
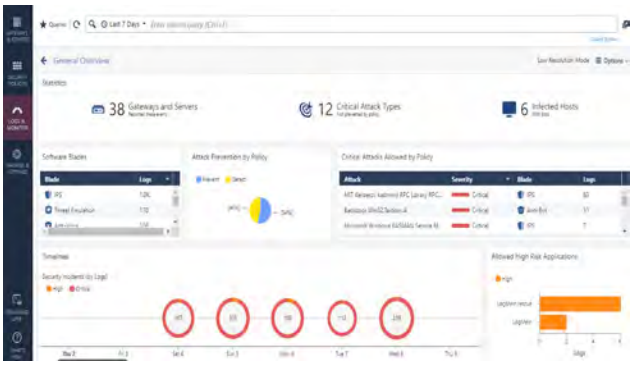
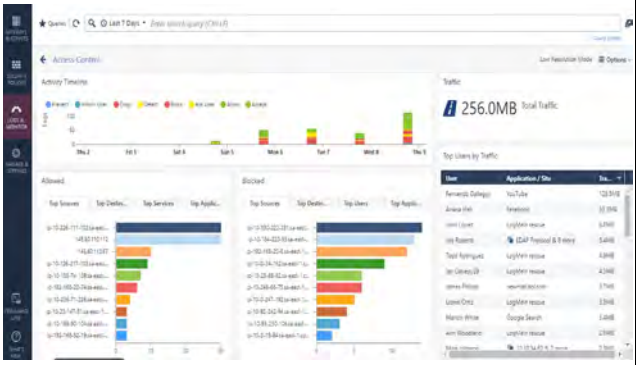
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			Report Output Location Report results are saved in subdirectories of the **Results** subdirectory of the SmartReporter server as follows: <Result Location>/<Report Name>/<Generation Data & Time> For each report, a directory with the report's name (for example, <Report Name>) is created in <Result Location>, with a subdirectory named with the generation date and time <Generation Date & Time>. The report is generated into this <Generation Date & Time> subdirectory. The result location can be modified by selecting **Tools > Options** and specifying the desired location in the **Result Location** field of the **Options** window's **Generation** page. In addition to saving the result to the SmartReporter server, you can send it to any of the following: ▪ The Client's display (the default setting). ▪ Email recipients. ▪ An ftp or a web server. See Uploading Reports to an FTP Server. ▪ Via a Custom Report Distribution script. The **Mail Information** page of the **Options** window allows you to specify both the sender's Email **Reports Tab** Use the **Reports** tab to see, manage and generate reports that show a summary of events identified by SmartEvent. You can generate report for these supported blades: ▪ Application and URL Filtering events ▪ Data Loss Prevention events ▪ IPS events ▪ Anti-Bot and Anti-Virus events ▪ **All** - Tabular list of all events, including events not related to these supported blades Each supported blade has its own filter criteria and format that for presenting the information. Each report contains a high-level summary of event patterns followed by detailed analyses and graphs. Each report has its own format and filter criteria. You can generate reports that show events on a daily, weekly or monthly basis. Some blades can show events summarized by domain. SmartEvent includes these output options for your generated reports: ▪ Show on the **Reports** tab ▪ Open in a Web browser ▪ Print ▪ Save as a PDF file ▪ Send as an email attachment to specified individuals	Verificado

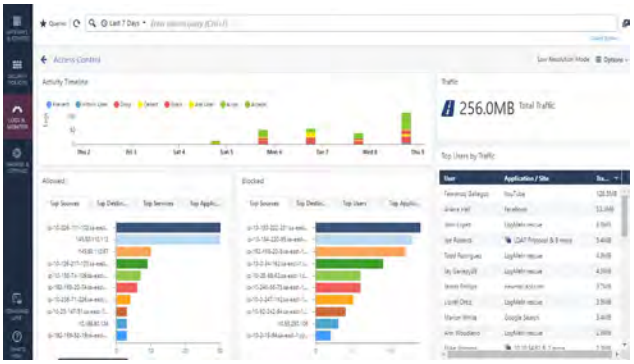
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			To configure email settings for each defined report: 1. Select a report in the **Reports** tree and click **Manage**. 2. Go to the **Email Settings** pane. 3. Select the **Send By Email** option (cleared by default). You must select this option to automatically send reports by email. 4. Select the **Custom** option. 5. Enter recipient email addresses in the **To** and **Cc** fields. You can enter many email addresses in each field, separated by a semicolon. 6. Select the **Report Format**: • **HTML** • **PDF** **MHT** - MIME HTML archive format	
18	Debe detectar ataques de denegación de servicio, correlacionando eventos de todas las fuentes.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
19	La consola de reportería o de administración debe tener la capacidad mostrar la matrix MITREK vs el evento de seguridad correlacionado.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	CP_R81_LoggingAndMonitoring_AdminGuide.pdf página 62, 63	Verificado
20	El sistema de información debe proporcionar información consolidada sobre:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	

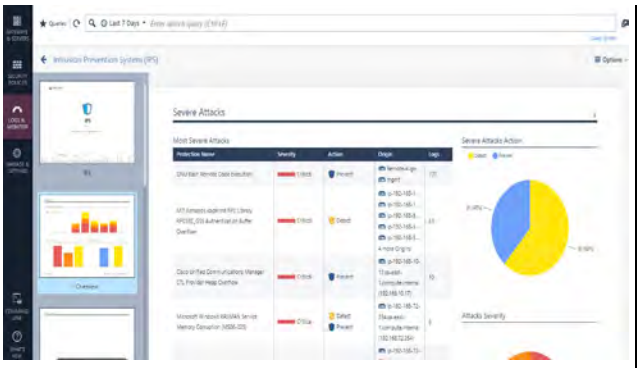
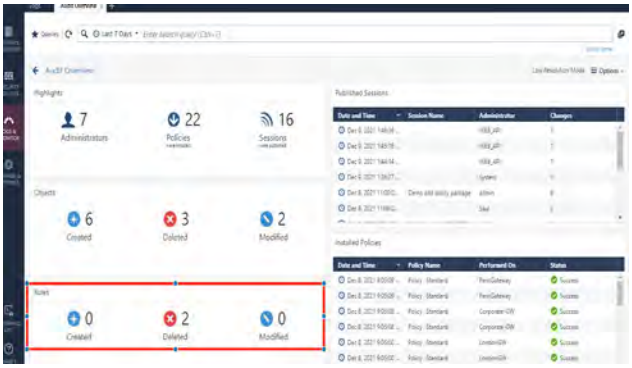
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

21	El volumen de conexiones que fueron bloqueados por la regla de seguridad.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	 	Verificado
22	Principales fuentes de conexiones bloqueadas, sus destinos y servicios	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

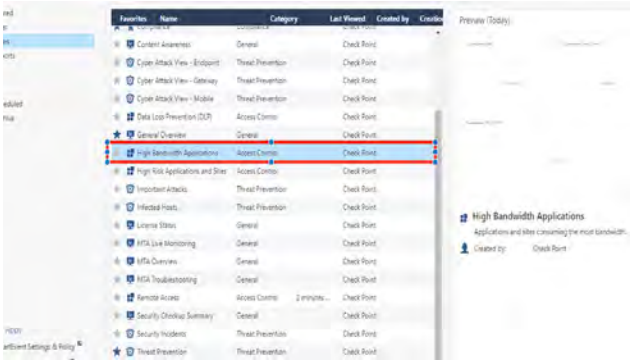
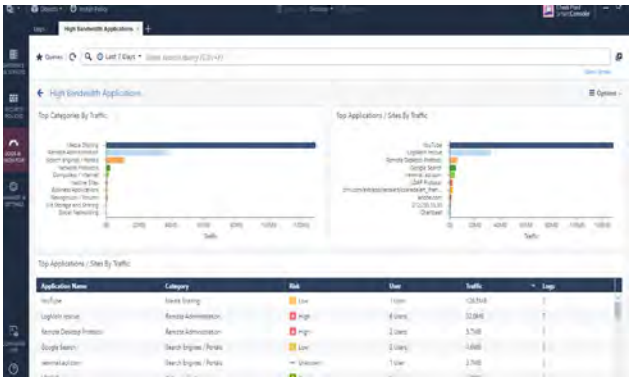
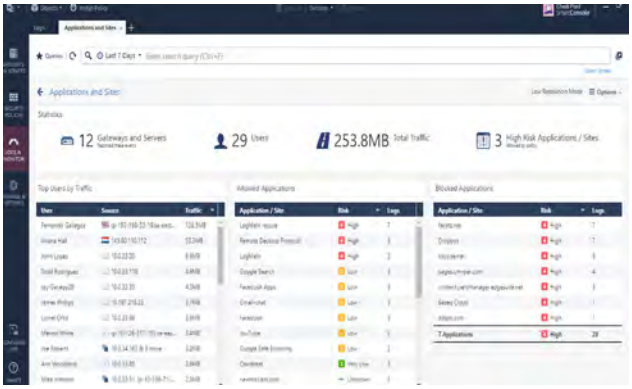
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

23	Top reglas utilizadas por la política de seguridad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
24	ataques de seguridad a nivel detectados por punto de aplicación (perímetro) que determinan sus principales fuentes y los destinos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

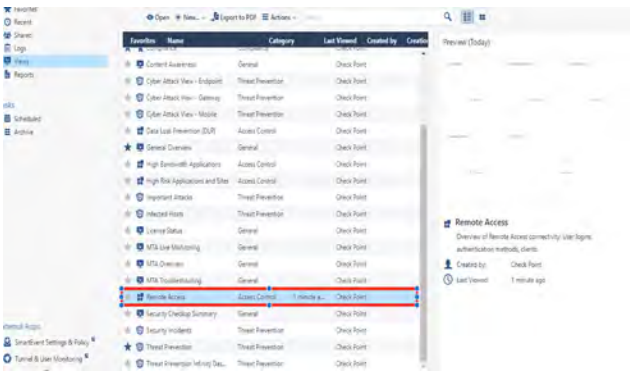
Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

				
25	Número de políticas instalar y desinstalar en el punto de aplicación	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
26	Top servicios de redes	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

27	actividad en la web por el usuario que detalla los principales sitios visitados y los usuarios de Internet top	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	  	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

				
28	Top servicios que crean la mayor parte de carga para el tráfico cifrado	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
29	Los mejores usuarios en VPN que realizan las conexiones de más larga duración	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	La solución ofrecida permite correlacionar eventos de usuarios de VPN y sus tiempo de conexión.	Verificado
R	**Mejor Práctica de Gobierno, Riesgo y Cumplimiento (GRC)**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	
1	La solución debe tener una modulo integrado de cumplimiento que permita supervisar los Gateway, las	**ENTERADOS, ACEPTAMOS Y**	Ver compliance-datasheet.pdf	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	políticas y ajustes de configuración de una manera dinámica y en tiempo real.	**CUMPLIMOS**		
2	La solución debe tener una módulo de cumplimiento que permita la supervisión de Cumplimiento en los diferentes módulos de seguridad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver compliance-datasheet.pdf	Verificado
3	La solución debe tener una módulo de cumplimiento que permita la evaluación en tiempo real de cumplimiento de las regulaciones principales de la industria (PCI-DSS, GDPR, HIPAA, SOX, ISO 27001, entre otros)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver compliance-datasheet.pdf	Verificado
4	La solución debe tener una módulo de cumplimiento que permita la notificación inmediata de los cambios de políticas que afecten el cumplimiento	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver compliance-datasheet.pdf	Verificado
5	La solución debe tener una módulo de cumplimiento que permita proporcionar recomendaciones prácticas para mejorar el cumplimiento	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver compliance-datasheet.pdf	Verificado
6	La solución debe tener una módulo de cumplimiento que permita recomendar Mejores prácticas de seguridad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver compliance-datasheet.pdf	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

7	La solución debe tener una módulo de cumplimiento que permita traducir los requisitos reglamentarios en las mejores prácticas de seguridad accionable	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver compliance-datasheet.pdf	Verificado
8	La solución debe tener una módulo de cumplimiento que permita el monitoreo en tiempo real de la puerta de enlace con las mejores prácticas de seguridad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver compliance-datasheet.pdf	Verificado
9	La solución debe tener una módulo de cumplimiento que permita generar informes de evaluación automatizada para calificar el cumplimiento de las regulaciones	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver compliance-datasheet.pdf	Verificado
10	La solución debe tener una módulo de cumplimiento que permita comprobar el cumplimiento de todos los cambios en las políticas para los diferentes módulos de seguridad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver compliance-datasheet.pdf	Verificado
11	Capacidades	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf**	Verificado
12	Soportar puerto para conexión de consola serial RJ-45	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 2, 3**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

13	Soportar al menos 1024 VLANs a nivel la solución.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 3**	Verificado
14	Cada appliance gateway debe tener al menos 8 interfaces 10G SFP+ en Fibra con sus respectivos transciever SFP+ y 8 interfaces 10/100/1000 en cobre y/o fibra con sus respectivos transciever SFP, un puerto asignado para la administración vía consola, un puerto para administración y sincronización o HA independiente a las 8 interfaces de cobre a 1G.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 2, 3**	Verificado
15	Cada appliance Gateway debe tener dos slot de expansión para intercambiar tarjetas de puertos, con la capacidad de colocar tarjetas de expansión de puertos de hasta 40GBase-F QSFP, con acceso frontal sin la necesidad de destapar todo el appliance.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 2, 3**	Verificado
16	Cada Appliance gateway debe tener almacenamiento de dos discos duros de al menos 480 GB Estado Solido cada uno.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 3**	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

17	La solución debe soportar 9.5 Gbps de throughput con todas sus funcionalidades activas por cada appliance gateway	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 3**	Verificado
18	La solución debe soportar 25 Gbps de throughput de IPS por cada appliance gateway	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 3**	Verificado
19	Cada appliance gateway debe soportar 22 Gbps de throughput de NGFW (FW, IPS, Control de aplicaciones)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 3**	Verificado
20	Cada appliance gateway debe manejar hasta 16 millones de conexiones concurrentes.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 3**	Verificado
21	Cada appliance gateway debe soportar 330 mil conexiones por segundo.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 3**	Verificado
22	Cada uno de los appliances gateway debe tener Doble fuente de poder hot-swap	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Ver **7000-security-gateway-datasheet.pdf página 2**	Verificado

ÍTEM	**REQUERIMIENTOS WAF**	**Cumple**	**REFERENCIA**	**Revisión**
		SI/NO		

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

A	REQUERIMIENTOS GENERALES			
1	Requerimiento	ENTERADOS, ACEPTAMOS Y CUMPLIMOS	Observación	
2	La solución de WAF y/o Application Delivery Controller con funcionalidades completas de WAF deberá estar ubicada en el cuadrante Leaders del informe Gartner Magic Quadrant de los últimos tres años, desde la última publicación registrada por Gartner.	ENTERADOS, ACEPTAMOS Y CUMPLIMOS	Figure 1. Magic Quadrant for Application Delivery Controllers  Source: Gartner (August 2016) 	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			De acuerdo a la observación realizada por SOFTSECURITY y aceptada por la UPN, la solución propuesta se encuentra en el cuadrante de Lideres de Gartner en los dos últimos años desde su ultima publicación, es decir en los años 2016 y 2015, adicionalmente tambien se encuentra como lider en los años 2013 y 2012.	
3	El equipo debe venir licenciado para soportar como mínimo un Throughput en L4/L7 de 6 Gbps	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Alteon_Master_TechSpec_12-2020.pdf Pág: 9, Performances	Verificado
4	El Equipo debe soportar crecimiento de throughput por licenciamiento sobre el mismo hardware de L4/L7 de 26/20 Gbps respectivamente. En caso de no soportar crecimiento a través de licenciamiento se	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Alteon_Master_TechSpec_12-2020.pdf Pág: 9, Performances	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	deberá incluir una capacidad mínima de throughput de 26 Gbps.			
5	El Equipo debe soportar como mínimo 625000 conexiones por segundo en capa 4.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Alteon_Master_TechSpec_12-2020.pdf Pág: 9, Performances	Verificado
6	El Equipo debe soportar como mínimo 50 Millones conexiones concurrentes en capa 4.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Alteon_Master_TechSpec_12-2020.pdf Pág: 9, Performances	Verificado
7	Capa equipo debe soportar como mínimo 845000 request por segundo en capa 7.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Alteon_Master_TechSpec_12-2020.pdf Pág: 9, Performances	Verificado
8	El equipo debe tener la siguiente capacidad en interfaces como mínimo (es necesario incluir los tranceivers en fibra):	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Alteon_Master_TechSpec_12-2020.pdf Pág: 9, HW Specification	Verificado
	- 8 puertos 1Gbps cobre y/o fibra	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- 2 puertos 10Gbps fibra (SR)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
9	El Equipo debe incluir un puerto de administración fuera de banda tipo RJ45 y	**ENTERADOS, ACEPTAMOS Y**	Alteon_Master_TechSpec_12-2020.pdf Pág: 9, Performances	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	otro USB para recovery.	**CUMPLIMOS**		
10	El Equipo debe incluir fuente de poder redundantes AC/DC hot swappable	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Alteon_Master_TechSpec_12-2020.pdf Pág: 9, HW Specification	Verificado
11	El Equipo debe incluir como mínimo un disco duro SSD de 500 GB de capacidad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Alteon_Master_TechSpec_12-2020.pdf Pág: 9, HW Specification	Verificado
12	La solución debe ser capaz de integrarse con herramientas de automatización del mercado solamente utilizando software proporcionado por el fabricante, incluyendo al menos:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Radware_vDirect_414_Integration_OpenStack.pdf Radware_vDirect_414_Integration_VMware_Orchestrator.pdf Radware_vDirect_414_Integration_Kubernetes.pdf https://galaxy.ansible.com/radware/radware_modules	Verificado
	OpenStack	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	Vmware vRealize Orchestrator	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	Cisco ACI	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	Ansible	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	Kubernetes	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
13	La solución debe incluir un REST API donde se provea acceso completo a la funcionalidad el equipo, incluyendo crear, leer, actualizar o borrar información.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Alteon_Master_TechSpec_12-2020.pdf Pág: 51-52, AppWall Management Application	Verificado
B	**REQUERIMIENTOS DE SWITCHING Y ROUTING**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		
1	La solución debe soportar link aggregation de acuerdo con el estándar 802.3ad, con capacidad de agregar hasta 8 puertos en físicos en un puerto lógico.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 148, LACP Overview	Verificado
2	La solución debe soportar LACP estático y dinámico	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 148-150, LACP Overview	Verificado
3	La solución debe soportar los siguientes protocolos de spanning tree:	**ENTERADOS, ACEPTAMOS Y**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 154, Multiple Spanning Trees Pág. 157, Rapid Spanning Tree Protocol	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		
	- Spanning Tree Protocol STP (802.1D)	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Rapid Spanning Tree RSTP (802.1w)	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Multiple Spanning Tree MSTP (802.1s)	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
4	La solución soporta como mínimo los siguientes tipos de NAT:	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 537-540, Network Address Translation	Verificado
	- Dinámico: NAT muchos a uno.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Estático: NAT uno a uno.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Overlapping: Misma dirección IP, pero en diferentes VLAN.	**ENTERA DOS, ACEPTA MOS Y**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		
5	La solución debe soportar como mínimo los siguientes protocolos de enrutamiento:	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 173, Routing Information Protocol Pág. 177, Border Gateway Protocol Pág. 183, Open Shortest Path First (OSPF)	Verificado
	- RIPv1 y RIPv2	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- BGP	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- OSPF y OSPFv3	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
C	**ADMINISTRACIÓN LOCAL DE LA PLATAFORMA**	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		
1	La solución debe soportar administración local vía SSH y WBM (Web Based Management) via HTTPS y debe permitir personalizar el certificado digital a presentar.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 156, Dedicated Management Port Pág. 74, Certificate Administrator	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

2	La solución debe permitir crear reglas de acceso a la administración a través de la definición de las IP que podrán acceder y especificando los protocolos de administración.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 58, Limiting Management Access	Verificado
3	La solución debe permitir especificar límites de tasa de tráfico sobre el tráfico de administración	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 58, Limiting Management Access	Verificado
4	La solución debe soportar autenticación local, RADIUS y TACACS+	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 70, RADIUS Authentication and Authorization Pág. 75, TACACS+ Authentication	Verificado
D	**REQUERIMIENTOS DE BALANCEO LOCAL DE SERVIDORES (SLB)**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		
1	La solución debe balancear el tráfico enviado desde los clientes a través de la exposición de un servicio virtual y posterior entrega del tráfico a un grupo de servidores reales a balancear.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 241, CHAPTER 11 – SERVER LOAD BALANCING	Verificado
2	La solución debe soportar las siguientes topologías IP	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 290-296, IPv6 and Server Load Balancing Pág. 241, CHAPTER 11 – SERVER LOAD BALANCING	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- IPv4 pura, con clientes y servidores reales en IPv4.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- IPv6 pura, con clientes y servidores reales en IPv6.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Clientes IPv4 y servidores en IPv6 o servidores IPv4 y clientes IPv6	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
3	La solución debe soportar balanceo transparente, en donde se realicé inspección del tráfico, clasificación y envío a uno o más grupos de balanceo, sin alterar el paquete original.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 516, Transparent Load Balancing	Verificado
4	La solución debe permitir filtrar el tráfico, permitiendo aceptar o denegar el mismo, utilizando como mínimo los siguientes parámetros:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 519, To redirect traffic with a transparent server Pág. 524, To redirect traffic with proxy server port address translation Pág. 526, To redirect traffic with a non-transparent server	Verificado
	- Dirección MAC.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Dirección IP.	**ENTERADOS, ACEPTAMOS Y**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		
	- Protocolo.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Banderas TCP.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Tipos de mensaje ICMP.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Puertos capa 4.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- String en Capa 7.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
5	La solución debe permitir configurar el máximo número de conexiones permitidas por servidor real.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 266, Maximum Connections for Real Servers	Verificado
6	La solución debe permitir configurar peso sobre los servidores para trabajar con algoritmos de	**ENTERA DOS, ACEPTA MOS Y**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 250, Physical and Logical Real Server Modes	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	balanceo basados en el peso otorgado.	**CUMPLIMOS**		
7	La solución debe modificar los pesos asignados de forma dinámica basada en resultados de monitoreo de salud enviados vía SNMP.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 265, Readjusting Server Weights Based on SNMP Health Check Response	Verificado
8	La solución debe permitir configurar un servidor real de backup para cada servidor real definido, el cual asumirá la carga en caso de que el servidor real principal falle.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 270, Secondary Backup Real Server Group	Verificado
9	La solución debe soportar la definición de servidores reales a través de su FQDN.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 296, FQDN Servers	Verificado
10	La solución debe soportar al menos los siguientes algoritmos de balanceo:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 260, Metrics for Real Server Groups	Verificado
	- Hash	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Persistent Hash	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Tunable Hash	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Weighted Hash	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Highest Random Weights	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Least Connections	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Least Connections Per Service	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Round-Robin	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Response Time	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Bandwidth	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
11	La solución debe soportar chequeos de salud para validar el estado de los servidores reales objetos de balanceo, soportando al menos los siguientes métodos predefinidos:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 477, CHAPTER 16 – HEALTH CHECKING	Verificado
	TCP, half-open TCP, ICMP, HTTP/S, DNS (TCP & UDP based), TFTP, SNMP, FTP, POP3, SMTP, IMAP, NNTP, RADIUS, SSL, LDAP/S, WAP, ARP, DHCP, RTSP	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
12	La solución debe permitir personalizar y crear nuevos chequeos de salud con base en los chequeos de salud predefinidos.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 477-506, CHAPTER 16 – HEALTH CHECKING	Verificado
13	La solución debe permitir crear nuevos chequeos de salud utilizando scripts	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 492, Script-Based Health Checks	Verificado
14	La solución debe permitir configurar chequeos de salud compuestos de chequeos individuales, a través de expresiones lógicas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 504-505, Advanced Group Health Check	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	La solución debe soportar balanceo por contenido HTTP de forma nativa y sin scripting adicional, utilizando al menos los siguientes elementos del protocolo HTTP para la creación de las reglas:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- URL hostname	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- URL Path	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
15	- URL Page name	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 552, Content Class Overview	Verificado
	- URL page Type	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Cualquier encabezado HTTP	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Cookies	**ENTERADOS, ACEPTAMOS Y**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		
	- Texto específico en el encabezado o en el cuerpo del mensaje.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- XML tags	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
16	La solución debe permitir la inclusión de la IP original del cliente en un header HTTP para preservar la IP en caso de NAT de cliente.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 321, Sending Original Client IP Addresses to Servers	Verificado
17	La solución debe permitir controlar los códigos de respuesta HTTP enviados por los servidores reales	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 322, Controlling Server Response Codes	Verificado
18	La solución debe permitir ocultar la información de identidad de los servidores HTTP balanceados, modificando las respuestas enviadas por los servidores reales.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 324, Enhancing Server Security by Hiding Server Identity Pág. 325, Enhancing Security by Hiding Page Locations	Verificado
19	La solución debe permitir modificaciones de contenido en las respuestas enviadas por los servidores o en las solicitudes realizadas por los	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 327, Advanced Content Modifications	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	clientes, de forma nativa, sin necesidad de script, en al menos los siguientes elementos HTTP:			
	- HTTP Headers: Podrán ser insertados, reemplazados o removidos.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Cookies	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- File Type	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Status Line	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- URL	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	-Text	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
20	La solución debe permitir la personalización de la entrega de aplicación a través de scripts	**ENTERADOS, ACEPTAMOS Y**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 842, CHAPTER 26 – APPSHAPE++ SCRIPTING	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	escritos por los usuarios.	**CUMPLI MOS**		
21	La solución debe soportar persistencia utilizando la dirección IP de origen.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 461, Source IP Address	Verificado
22	La solución debe soportar persistencia a través de cookie utilizando los siguiente métodos:	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 464, Cookie Modes of Operation	Verificado
	- Cookie Insert.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Cookie Re-write.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Cookie Passive.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
23	La solución debe soportar persistencia basada en cualquier parámetro del header o el cuerpo del mensaje HTTP, incluyendo Tags de XML	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 470, Server-Side Multi-Response Cookie Search	Verificado
24	La solución debe soportar persistencia	**ENTERA DOS, ACEPTA MOS Y**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 470, SSL Session ID	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	a través de SSL Session ID.	**CUMPLIMOS**		
25	La solución debe soportar persistencia a través de SIP Call ID.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 472, SIP Call ID	Verificado
26	La solución debe soportar persistencia en Windows Terminal Server	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 473, Windows Terminal Server Load Balancing and Persistence	Verificado
27	La solución debe soportar persistencia para cualquier protocolo TCP/UDP a través de scripting.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 482, CHAPTER 26 – APPSHAPE++ SCRIPTING	Verificado
E	**REQUERIMIENTOS DE OPTIMIZACIÓN GENERAL**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		
1	La solución debe soportar caching conforme al RFC 2616	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 352, Content-Intelligent Caching	Verificado
2	La solución debe utilizar la memoria RAM para almecenar el contenido "cacheado" y la cantidad de RAM destinada para el cache podrá ser definida en la configuración.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 354-355, Content-Intelligent Caching	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

3	La solución debe incluir la funcionalidad de compresión HTTP	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 356, Content-Intelligent Compression	Verificado
4	La funcionalidad de compresión deberá soportar al menos los siguientes algoritmos de compresión:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 356, Content-Intelligent Compression	Verificado
	- gzip	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Deflate	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
5	La solución debe soportar HTTP multiplexing incluso si el servicio virtual se encuentra configurado con SSL offloading, caché y compresión.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 361, HTTP Multiplexing	Verificado
6	La solución debe soportar TCP pooling para mejorar el overhead que impone el establecimiento y terminación de las conexiones TCP con los servidores reales.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 362, Pooling	Verificado
7	La solución debe permitir definir políticas de optimización TCP que se podrán aplicar de forma independiente a la	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 362, FastView for Alteon	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	comunicación de cara al cliente y a la comunicación de cara al servidor.			
8	La solución debe soportar HTTP/2 Gateway, con la conexión de cara al cliente en HTTP/2 y de cara al servidor en HTTP 1.1	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 364, HTTP/2 Support	Verificado
9	La solución debe soportar HTTP/2 Full Proxy con cliente y servidor en HTTP/2.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 364, HTTP/2 Support	Verificado
10	La solución debe soportar aceleración a través de SSL offloading como mínimo para los siguientes protocolos:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 435, Virtual Service or Filter	Verificado
	- HTTPS	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- SSL Genérico	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- SIP	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- SMTP (STARTTTLS)	**ENTERADOS, ACEPTAMOS Y**		

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		Verificado
	- IMAP (STARTTTLS)	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- POP3 (STARTTTLS)	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- LDAP (STARTTTLS)	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- FTPS	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
11	La solución debe soportar SSLv3, TLSv1, TLSv1.2, TLSv1.3	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 912, Main Ciphers	Verificado
12	La solución debe soportar SNI para mantener múltiples hosts detrás de una única IP y puerto.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 302, Content-Intelligent Server Load Balancing	Verificado
13	La solución debe soportar FIPS 140-2 Level 3, a través del uso de un HSM integrado	**ENTERA DOS, ACEPTA MOS Y**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 444, Internal HSM Card	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		
14	La solución debe soportar HSM de red y ser compatible con SafeNet Luna Network HSM 7 de Gemalto/Thales	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 446, Network HSM	Verificado
15	La solución debe contar como mínimo con el siguiente desempeño de SSL:	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Alteon_Master_TechSpec_12-2020.pdf Pág. 9, Performance - RSA CPS (llaves de 2K): 20,5K - ECC CPS (P256): 12K - SSL Throughput (Gbps): 10	Verificado
	- RSA CPS (llaves de 2K): X	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- ECC CPS (P256): Z	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- SSL Throughput (Gbps): W	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
F	**REQUERIMIENTOS DE OPTIMIZACIÓN DE DESEMPEÑO EN CAPA DE APLICACIÓN WEB**	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		
1	La optimización de desempeño WEB debe permitir trabajar en un modo aprendizaje, en donde no se apliquen	**ENTERA DOS, ACEPTA MOS Y**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 369, TCP Optimization Policies	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	las técnicas configuradas, pero si se pueda probar el sitio a través de una URL específica.	**CUMPLIMOS**		
2	La solución debe soportar PUSH Automático en HTTP/2, basado en el análisis del sitio, para enviar los recursos al navegador tan rápido como sea posible.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 363, Server PUSH	Verificado
3	La solución debe soportar técnicas de aceleración específicas para dispositivos móviles	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 302, Content-Intelligent Server Load Balancing	Verificado
4	La solución debe soportar optimización específica por tipo de navegador.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-x-FastView-Alteon-UG.pdf Pág. 43, Dynamic Browser Caching	Verificado
5	La solución debe soportar Predictive Browser Caching permitiendo precargar recursos del sitio web para acelerar la carga del mismo.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-x-FastView-Alteon-UG.pdf Pág. 43, Dynamic Browser Caching	Verificado
6	La solución debe soportar la consolidación de los siguientes recursos dinámicos:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-x-FastView-Alteon-UG.pdf Pág. 43, Dynamic Resource Consolidation	Verificado
	- Consolidación de CSS.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Consolidación de Javascripts	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Consolidación de Imágenes.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
7	La solución debe soportar el rendering progresivo de las imágenes, permitiendo comprimir las imágenes, cargarlas en una resolución menor y luego mejorarla una vez la página haya sido cargada.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-x-FastView-Alteon-UG.pdf Pág. 43, Payload Reduction	Verificado
8	La solución debe soportar compresión de imagenes usando configuración específica para cada dispositivo: Desktop, Dispositivos Móviles y Tabletas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-x-FastView-Alteon-UG.pdf Pág. 43, Payload Reduction	Verificado
G	**REQUERIMIENTOS DE BALANCEO GLOBAL**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		
1	La solución debe permitir el balanceo de tráfico a través de múltiples sitios físicos.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 39, CHAPTER 2 – BASIC LINK LOAD BALANCING	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

2	La solución debe permitir redirección global basada en los siguientes métodos: DNS, HTTP y Proxy (NAT de los clientes) para las aplicaciones que no usen DNS ni sean HTTP.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 1028, APPENDIX G – LEGACY LAYER 7 DNS LOAD BALANCING	Verificado
3	La redirección DNS debe soportar DNSSEC	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 1028, APPENDIX G – LEGACY LAYER 7 DNS LOAD BALANCING	Verificado
4	La solución debe monitorear el estado de los balanceadores en sitios remotos, como mínimo:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 45, DNS Response Parameters	Verificado
	- Tiempo de repsuesta de los servidores	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Uso de la CPU	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Disponibilidad y uso de de sesiones	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
5	La solución debe soportar como mínimo las siguientes reglas de balanceo global:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 46, Link Selection Metrics	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Red o redes de origen.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Ubicación geográfica.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Menor número de conexiones.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Roundrobin	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Weighted Roundrobin	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Menor tiempo de repuesta	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Combinación de tiempo de respuesta y menor número de conexiones.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Ancho de banda	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Proximidad, midiendo el tiempo de respuesta entre cada datacenter y el cliente	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Persistencia	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Hash de la IP de origen y el nombre del dominio	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
6	La solución debe permitir la configuración de balanceo global, aún estando detrás de un dispositivo que realice un NAT de las direcciones IP públicas como un Firewall y no debe requerir hardware adicional para realizar esto.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 41, Smart NATLink Selection Metrics	Verificado
H	**REQUERIMIENTOS DE BALANCEO DE ENLACES**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

1	La solución debe soportar balanceo de enlaces para tráfico entrante y para tráfico saliente.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 33, CHAPTER 1 – OVERVIEW	Verificado
2	El balanceo de enlaces debe contar con al menos las siguientes opciones de despliegue:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 33, CHAPTER 1 – OVERVIEW	Verificado
	- Capa 3 o modo ruteo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Capa 2 o modo bridge	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
3	La solución debe permitir definir los enlaces a balancear especificando:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 39, WAN Links	Verificado
	- Dirección IP del router de upstream.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Chequeo de salud por enlace.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- NAT a configurar para el balanceo de salida	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
4	La solución debe permitir configurar reglas de balanceo de salida que permitan clasificar el tráfico y balancearlo de acuerdo a las características del mismo.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 40, Outbound Link Load Balancing	Verificado
5	El balanceo de enlaces de salida debe permitir clasificar el tráfico con al menos los siguientes parámetros:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 40, Outbound Link Load Balancing	Verificado
	- Vlan	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Dirección IP Origen/destino	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Puerto Origen/Destino	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Protocolo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Contenido a capa 7	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Estático definiendo los grupos por donde se debe enviar el tráfico	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
6	La solución debe contar con al menos las siguiente métricas en el balanceo de salida para determinar el mejor enlace:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 46-47, Link Selection Metrics	Verificado
	- Least Connections	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Round-Robin	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Response Time	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Bandwidth	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	La solución debe soportar al menos los siguientes tipos de conversiones de direcciones de red (NAT):	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- No NAT: que el tráfico se reenvíe de forma transparente	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
7	- NAT dinámico	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 40, Smart NAT	Verificado
	- NAT estático	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- NAT de prefijos de IPv6	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
8	En cuanto al balanceo de enlaces entrante, la solución debe actuar como un DNS autoritativo para las URLs balanceadas	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 44, DNS Authority	Verificado
9	La solución debe soportar al menos los siguientes tipos de records: A, AAAA y PTRs.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 44, DNS Authority	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	La solución debe soportar al menos las siguientes métricas para el balanceo de enlaces entrante:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Red o redes de origen.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Ubicación geográfica.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
10	- Menor número de conexiones.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 46, Link Selection Metrics	Verificado
	- Roundrobin	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Weighted Roundrobin	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Menor tiempo de repuesta	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Combinación de tiempo de respuesta y menor número de conexiones.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Ancho de banda	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Persistencia	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Hash de la IP de origen y el nombre del dominio	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
11	La solución debe incluir una métrica por proximidad que correlacione la latencia y el número de saltos hacia un origen determinado, para el balanceo de salida y desde un origen determinado para el balanceo entrante.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-LinkProof-for-Alteon.pdf Pág. 49, Proximity	Verificado
I	**REQUERIMIENTOS DE VIRTUALIZACIÓN**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		
1	La solución debe soportar instancias virtuales de balanceo que se ejecuten sobre un hypervisor	**ENTERADOS, ACEPTAMOS Y**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 91, vADCs	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	de balanceo especializado.	**CUMPLIMOS**		
2	La propuesta debe incluir como minimo con 5 balanceadores virtuales con capacidades de WAF y con posibilidad de crecimiento hasta 22 instancias sin necesidad de modificar el hardware propuesto.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Alteon_Master_TechSpec_12-2020.pdf Pág: 9, Licenceses	Verificado
3	La solución debe soportar administración independiente para cada uno de los balanceadores virtuales configurados.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	Alteon_Master_TechSpec_12-2020.pdf Pág: 92, vADC Management	Verificado
4	Las solución debe permitir asignar recursos físicos independientes, CPU, Memoria, sobre cada instancia virtual y WAF; los recursos físicos asignados no debe compartirse entre las instancias virtuales de balanceo.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 91-93, vADCs	Verificado
5	La solución debe permitir que cada balanceador virtual maneje su propia infraestructura de red independiente, tanto en capa 2 como en capa 3, incluyendo protocolos de enrutamiento dinámicos.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 92, Figure 20: Network Architecture Configured to use ADC-VX	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

6	La solución soporta múltiples imágenes de software por cada balanceador virtual. Cada balanceador podrá correr una imagen de software distinta.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 91-93, vADCs	Verificado
7	La solución debe permitir realizar actualización sobre una instancia virtual sin afectar las otras instancias virtuales aprovisionadas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 91-93, vADCs	Verificado
8	La solución debe permitir asignar recursos físicos independientes para la funcionalidad de Optimización de desempeño Web.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 91-93, vADCs	Verificado
9	La solución debe permitir asignar recursos físicos independientes para la funcionalidad de Web Application Firewall, para evitar que el balanceador y el WAF comportan los mismos recursos.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 91-93, vADCs	Verificado
J	**REQUERIMIENTOS DE SEGURIDAD**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		
1	La solución debe soportar ACL (listas de control de acceso) para controlar el acceso a los dispositivos que conforman la solución y a los servidores balanceados	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 708, IP Address Access Control Lists (ACLs)	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

2	La solución debe permitir configurar rate limits en TCP, UDP e ICMP.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 718, Protocol-Based Rate Limiting	Verificado
3	La solución debe permitir configurar manualmente patrones de ataques y luego crear reglas de bloqueo de tráfico TCP o UDP, basadas en dichos patrones de tráfico.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 788, CHAPTER 25 – REPORTING	Verificado
4	La solución debe permitir generar y enviar alertas vía syslog y snmp, a otros dispositivos de seguridad, cuando se superen, como mínimo, los siguientes thresholds:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 788, CHAPTER 25 – REPORTING	Verificado
	- Ancho de banda.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Conexiones por Segundo.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Latencia.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Paquetes por segundo.	**ENTERADOS, ACEPTAMOS Y**		

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		Verificado
5	La solución debe incluir IP reputation, con configuración de acciones, Alertar, Permitir y bloquear, de acuerdo con:	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 197, Signature Update Service (SUS)	Verificado
	- La región (ubicación)	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- La categoría: Tor Exit Nodes e IP Maliciosas	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- El nivel de riesgo.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
6	El balanceador debe contar con la posibilidad de integración nativa a futuro con un servicio de administración de bots (Bot Management) del mismo fabricante, con las siguientes características mínimas:	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 750, Bot Manager Integration with Alteon	Verificado
	- Configuración por servicio virtual.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Soportar aplicaciones WEB, aplicaciones móviles y API.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Soportar análisis de comportamiento para análisis de intención, inteligencia colectivida de bots, fingreprinting de browsers y de máquinas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Permitir desde el balanceador, configurar al menos las siguientes respuestas ante ataques detectados: Permitir, Captcha, Bloqueo.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
K	**REQUERIMIENTOS DE INSPECCIÓN SSL**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**1**	
1	La solución debe proveer visibilidad SSL/TLS para ambos, el tráfico hacia el Datacenter y el tráfico saliente a Internet, permitiendo a la solución ser la responsible de la orquestación y distrubución dinámica de tráfico entre dispositivos de seguridad.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 735, SSL Inspection	Verificado
2	La solución de inspección SSL debe soportar al menos los siguientes tipos de despliegue:	**ENTERADOS, ACEPTAMOS Y**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 736, Deployment Modes	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		
	- Solución transparente en capa 2.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Dispositivo en modo ruteo en capa 3.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
3	En cuanto al número de dispositivos, la solución deberá poder desplegarse:	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	Alteon_Master_TechSpec_12-2020.pdf Pág: 9, Licenceses Security Inspection Devices	Verificado
	- Solución de una sola instancia.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Solución con dos (2) instancias utilizando dos equipos físicos o dos instancias virtuales	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
4	La solución debe ser agnostica a los dispositivos de seguridad conectados y debe soportar como mínimo, los siguientes tipos de dispositivos de acuerdo a su tipo de despliegue de red:	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 737, Security Inspection Devices	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Dispositivos en capa 3, que pueden estar conectados en one-leg o two-legs. Ejemplos: Antimalware, Firewalls.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Dispositivos en capa 2 conectados en two-legs. Ejemplo: ATP, IPS.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Dispositivos pasivos en donde solo secopie el tráfico, como DLPs e IDS. Conectados en one-leg.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- La solución debe soportar dispositivos tipo ICAP, como DLP activos y anti-virus.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
5	La solución para la inspección SSL de salida debe soportar Proxy Transparente y Proxy Explícito.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 739, Transparent or Explicit HTTPS Proxy	Verificado
6	La solución para la inspección SSL debe soportar bypass de inspección SSL la cual podrá definirse como mínimio a través de:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 739, Inspection Bypass	Verificado
	- Dirección IP origen o destino.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Sitios específicos o categorias.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
		ENTERADOS, ACEPTAMOS Y CUMPLIMOS		
	Se debe incluir todo el licenciamiento.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
7	La solución para la inspección SSL de salida debe detectar tráfico HTTPS y enviar para inspección en:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 739, Dynamic Port Discovery	Verificado
	- Un puerto específico definido	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Rango de puertos TCP.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Cualquier puerto TCP.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	La solución debe soportar la inspección de protocolos distintos a HTTP y que sean transportados sobre SSL/TLS:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
8	- Conexiones SSL/TLS - SSL/TLS explícitas, solicitadas vía STARTTLS para SMTP, IMAP y POP3 y AUTHTLS para FTP.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 740, Inspecting non-HTTPS protocols	Verificado
	- Conexiones implicitas SSL, cualquier tráfico no-http.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
9	La solución debe soportar múltiples grupos de dispositivos de seguridad en la cadena de inspección.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 741, Defining Inspection Tools Groups	Verificado
10	La solución debe permitir agrupar los dispositivos de seguridad y balancear el tráfico hacia los dispositivos definidos en los grupos.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 741, Defining Inspection Tools Groups	Verificado
11	La solución debe permitir crear políticas de inspección que definan a que grupos de dispositivos de seguridad se debe enviar el tráfico a ser inspeccionado.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 741, Defining SSL Policies	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

12	La solución debe permitir crear políticas que permitan manejar el tráfico que NO debe ser inspeccionado, por ejemplo, el tráfico en texto plano.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-CLI_Application_Guide.pdf Pág. 741, Defining SSL Policies	Verificado
L	**REQUERIMIENTOS DE WAF**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	**1**	
1	La solución debe incluir protección contra ataques en capa de aplicación WEB, WAF, y dicho WAF debe estar certificado por ICSA LABS	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 34, Overview https://www.icsalabs.com/vendor/radware-ltd	Verificado
2	La solución debe ofrecer protección de aplicaciones WEB contra amenazas registradas OWASP Top Ten vulnerabilities.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 36, OWASP Top Ten Vulnerabilities Classification	Verificado
3	La solución propuesta debe proteger contra ataques conocidos y ataques de día cero, soportando modelos de seguridad positivos y modelos de seguridad negativos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	https://www.radware.com/products/appwall/ What Does AppWall Do?	Verificado
4	La solución propuesta debe proteger contra mínimo los siguientes ataques en capa de aplicación WEB:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 38, WASC Web Security Attack Classification	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- XSS	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- SQL injections	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- OS command injections	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- LDAP injections	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- SSI injections	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- XPath injections	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Sensitive information leakage	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Application DoS	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- CSRF	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Parameter tampering	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- From field manipulation	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Session hijacking	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Cookie poisoning	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Application buffer overflows	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Brute Force attacks	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Access to predictable resource locations	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Unauthorized navigation	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Web server reconnaissance	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Directory/path traversal	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Forceful browsing	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Hotlink	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- HTTP response splitting	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Evasion and illegal encoding	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- XML validation	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Web services method restrictions and validation	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- HTTP RFC violations	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- HTTP request format and limitation violations	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Use of revoked or expired client certificates	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- File upload violations	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Clickjacking	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
5	La solución debe incluir una suscripción que permita actualizar las firmas de ataques conocidos, base de datos de geolocalización e IP de proxies anónimos.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 197, Signature Update Service (SUS)	Verificado
6	La solución debe permitir configurar una página de bloqueo interna o utilizar una página de bloqueo externa por cada aplicación configurada	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 166, Landing Pages	Verificado
7	La solución debe soportar los siguientes modos operacionales por cada aplicación configurada:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 76, Setting Tunnel Operation Modes	Verificado
	- Modo Reporte	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Modo Bloqueo	**ENTERADOS, ACEPTAMOS Y**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		
	- Modo bypass	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
8	La solución debe incluir un mecanismo que permita priorizar los recursos de procesamiento otorgados a las aplicaciones más críticas	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 154, AppWall Protection Against CORS Attacks	Verificado
9	La solución debe permitir los hostnames (virtual hosts) asociados a una aplicación, permitiendo usar wildcards en la definición de los hostnames y configurar políticas de seguridad por cada virtual host configurado	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 147, Prevention of CSRF (Cross Site Request Forgery) attack in AppWall, Hotlink Protection	Verificado
10	La solución debe controlar el tiempo timeout de conexión de los clientes a nivel TCP, definiendo para cada aplicación protegida el TCP Timeout de la sesión.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 168, Fingerprints Global Settings	Verificado
11	La solución debe controlar el tiempo timeout de conexión de los clientes a nivel HTTP, definiendo para cada aplicación protegida:	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 67, Table 8: HTTP Properties - General HTTP Properties	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- El tiempo que espera por datos de request del cliente.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- El tiempo que espera por una respuesta por parte del servidor.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
12	La solución debe bloquear queries con valores de parámetros definidos, pero sin un nombre de parámetro asociado al valor (NULL parameter name).	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 68, Table 9: HTTP Properties - Request Message (cont.) - Support parsing to NULL_PARAMETER _NAME of values when query parameter names are null	Verificado
13	La solución debe permitir purgar múltiples slashes en las urls y cambiarlos por un solo slash. Este comportamiento podrá ser modificado por cada aplicación.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 68, Table 9: HTTP Properties - Request Message (cont.)- Purge Multiple Slashes	Verificado
14	La solución debe permitir analizar las cookies como parámetros restringiendo el tamaño y los caracteres permitidos dentro de ellas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 68, Table 9: HTTP Properties - Request Message (cont.)- Analyze Cookies as Parameters	Verificado
15	La solución debe bloquear métodos que no estén en compliance con el RFC HTTP (rfc 2616)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 68, Table 9: HTTP Properties - Request Message (cont.)- Allow Non-RFC Compliant HTTP Methods	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

16	La solución debe proteger contra ataques de denegación de servicio de tipo low and slow a través de análisis de comportamiento	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 41, Table 3: AppWall Threat Protection - Low and Slow protection	Verificado
17	La solución debe permitir reemplazar los mensajes de respuesta HTTP por mensajes personalizados por cada aplicación protegida.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 70, Custom Headers	Verificado
18	La solución debe configurar los tamaños de mensajes permitidos para los requerimientos del cliente y las respuestas enviadas por el servidor, permitiendo definir como mínimo:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 73, Table 10: HTTP Properties - Reply Message (cont.)- Replace the HTTP Reply Messages with Custom Messages	Verificado
	- El tamaño del cuerpo del mensaje	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- El tamaño total de los encabezados	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- El tamaño total de un solo encabezado	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- El tamaño total de headers individuales.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
19	La solución debe permitir configurar listas blancas, listas negras de direcciones IP y políticas por geolocalización.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 67, Table 8: HTTP Properties - General HTTP Properties	Verificado
20	La solución debe contar con un mecanismo de bloqueo por origen que cuente con las siguientes características mínimas:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 168, Fingerprints Global Settings	Verificado
	- Debe hacer seguimiento a los ataques generados por una dirección IP en particular.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Debe hacer seguimiento a los ataques generados por un fingerprinting de dispositivo particular.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Dependiendo al nivel de ataque, la IP o el Fingerprinting serán bloqueados por un tiempo en minutos configurable.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Las IP o los fingerprinting de los dispositivos se podrán desbloquear desde el WBI de la solución	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

21	La solución debe enviar las IP bloqueadas por el mecanismo de source blocking a un mitigador de ataques DDoS del mismo fabricante, para que este efectúe el bloqueo en el perímetro	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 79, Deploying AppWall with DefensePro	Verificado
22	La solución debe descubrir de forma automática y a través del tráfico que cursa a través de ella, la estructura de cada aplicación web configurada.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.169, Auto Policy Generation	Verificado
23	La solución debe incluir un mécanismo de generación automática de política basado en el auto descubrimiento y en un análisis de amenazas realizado sobre los paths descubiertos.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.169, Zero Day Attack Blocking - Extended Mode	Verificado
24	El mécanismo de generación automática de políticas debe realizar como mínimo las siguientes acciones sin intervención humana:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.176, Auto Discovery	Verificado
	- Generar automáticamente los paths de cada aplicación	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Configurar las protecciones para cada path configurado	**ENTERADOS, ACEPTAMOS Y**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		
	- Refinar las protecciones	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Cambiar las protecciones de modo monitoreo a modo bloqueo	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
25	La solución debe continuar auto descrubriendo el sitio, modificando la política de seguridad y refinando las protecciones, aun estando sus protecciones en modo bloqueo	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.176, Auto Tunnel Settings Optimization	Verificado
26	La generación automática de políticas también debe ser capaz de ajustar automáticamente parámetros del protocolo HTTP, como mínimo:	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.176, Auto Tunnel Settings Optimization	Verificado
	-Definición del tamaño de los mensajes HTTP permitidos.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	-Las propiedades de parsing del protocolo HTTP en URLs específicas o de forma global	**ENTERA DOS, ACEPTA MOS Y**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		
27	La solución debe permitir definir los métodos permitidos hacia una determinada aplicación o path dentro de la aplicación	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.103, HTTPMethods Security Filter	Verificado
28	La solución debe contar con una protección que evalue las solicitudes de los clientes y bloquee aquellas que no hagan match con las expresiones definidas, las cuales deben contar como mínimo con las siguientes opciones de configuración	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.125, Session Security Filter	Verificado
	- host	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Path dentro de la aplicación	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Método HTTP	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Página	**ENTERA DOS, ACEPTA MOS Y**		

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		Verificado
	- Expresión Regular	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
29	La solución debe contar con una protección contra ataques de fuerza bruta que bloquee intentos de atacantes de hallar el usuario y password de un usuario autorizado.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.90, BruteForce Security Filter	Verificado
30	La protección contra ataques de fuerza bruta debe validar las respuestas de autenticación enviadas por los servidores WEB y bloquear la IP origen en caso que se genere un número configurable de respuestas de autenticación invalidas.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
31	La solución debe usar un motor de análisis de consulta de base de datos para detectar comandos de tipo SQL que los hackers puedan usar para realizar una manipulación de datos.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.95, Database Security Filter	Verificado
32	La solución debe permitir crear reglas para controlar el upload de archivos	**ENTERA DOS, ACEPTA MOS Y**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.97, FilesUpload Security Filter	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	con al menos los siguientes parámetros:	**CUMPLI MOS**		
	- Path de la aplicación.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Extensión del archivo	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Método HTTTP	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Permitir descarga de los archivos	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
33	La solución debe evaluar las respuestas de los servidores para determinar si estas están exponiendo información sensible, con al menos las siguientes características:	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.108, SafeReply Security Filter	Verificado
	- Debe redirigir a página de bloqueo o ocultar los caracteres, si la respuesta del servidor incluye información de tarjetas de crédito.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Debe redirigir a página de bloqueo o ocultar los caracteres, si la respuesta del servidor incluye un parámetro personalizado por el administrador a través de expresiones regulares.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
34	La solución debe incluir protección contra ataques dirigidos a WebServices, filtrando los compontes del WebService y validando cada uno de estos a través los distintos mécanismos de seguridad.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.111, WebServices Security Filter	Verificado
35	La solución debe validar las operaciones SOAP detectando ataques de tipo diccionario, codificaciones, manipulación de estructuras y otras amenazas comunes, como inyección de SQL y manipulación de parámetros.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.111, WebServices Security Filter	Verificado
36	La solución debe permitir importar el archivo WSDL y proveer al menos tres (3) niveles de validación:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.112-114, Configuring the WebServices Security Filter	Verificado
	- Validar que la estructura del XML esté correcta.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Validar el XML y asegurar que los requerimientos usen operaciones permitidas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Validar la estructura XML, la operación y que los mensajes estén en cumplimiento con los requerimientos definidos en el WSDL	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
37	La solución debe analizar XML en una solicitud, extraer los valores y pasar la información por otros mécanismos de seguridad, para detectar y mitigar ataques	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág.112-114, Configuring the WebServices Security Filter	Verificado
38	La solución debe soportar protección a API permitiendo importar el documento de OpenAPI y proveer:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 155, API Security	Verificado
	- Visibilidad sobre los endpoints definidos.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Permitir unicamente el tráfico que haga match con los endpoints definidos en el documento.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- El tráfico permitidos debe validarse por los otros mecanismos de seguridad de la solución.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Administración de cuota por cada endpoint definido.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
39	La solución debe permitir evaluar parámetros dentro de una solicitud de usuario detectando y bloqueando aquellas que no sean validas de acuerdo a los siguientes críterios que podrán ser configurados:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 121-124, Setting Query Parameters	Verificado
	- Tipo de parámetro: Long, Float, Número, Letra, Alfa númerico, Expresión, Cadena, Null Parameter.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Longitud mínima.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Longitud máxima.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Si permite o no valores nulos.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
40	La solución debe permitir bloquear el acceso a path específicos dentro de la aplicación	**ENTERADOS, ACEPTAMOS Y**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 43, Table 3: AppWall Threat Protection (cont.)- Path Blocking Security Filter	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		
41	La solución debe permitir cifrar la información de cookies para mitigar ataques que busquen manipular el estado de la sesión	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 125, Cookie Manipulation Protection	Verificado
42	La solución debe permitir cifrar la información en parámetros de tipo form, path y query para bloquear ataques que busquen manipular el estado de la sesión	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 125, Session Security Filter	Verificado
43	La solución debe incluir una base de datos de firmas de vulnerabilidades conocida.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 197, Signature Update Service (SUS)	Verificado
44	La solución debe permitir crear patrones personalizados para que sean validados junto con los incluidos en la base de datos de firmas de ataques conocidos.	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 197, Signature Update Service (SUS)	Verificado
45	La solución debe permitir configurar protección contra ataques de tipo Directory Listing para un grupo de hosts o para un host en particular	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 148, Directory Listing	Verificado
46	La solución debe permitir ofuscar la estructura real de la aplicación de un	**ENTERA DOS, ACEPTA MOS Y**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 148, URL Rewrite	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	atacante potencial a través de la configuración de reescritura de la URL (URL Rewrite)	**CUMPLIMOS**		
47	La solución debe soportar device fingerprinting para realizar seguimiento a las actividades utilizando un identificador de dispositivo y no la dirección IP origen.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 151, Device Fingerprinting	Verificado
48	La solución debe detectar bots de tipo motores de busqueda para excluirlos de la lista de origenes a los cuales se les hará seguimiento.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 167, Bot List	Verificado
49	La solución debe registrar al menos los siguientes eventos de auditoría:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 194, Configuration Audit Log	Verificado
	- Modificaciones de configuración.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Intentos de acceso no autorizados.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Reinicios de la solución o servicios.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	La solución debe registrar los eventos de seguridad detectados o bloqueados incluyendo como mínimo la siguiente información:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Severidad del evento	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Fecha	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
50	- Descripción corta del evento	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 182, Table 70: Log Examples	Verificado
	- El tipo de ataque.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Dirección IP origen	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Geolocalización	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Puerto Origen	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Host	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Path de la aplicación	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- URI	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Nombre del Parámetro	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Valor del Parámetro	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Tipo de Parámetro	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

51	La solución debe permitir refinar las políticas desde la vista de los eventos de seguridad.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 183, Working with the Security Log	Verificado
52	La solución debe permitir visualizar, para cada evento registrado, el header HTTP de la solicitud.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AlteonOS-32-6-6-AppWall_for_Alteon_UG.pdf Pág. 186, Displaying Graphical Reports of Applications and Security Filters	Verificado
53	La solución debe permitir visualizar, para cada evento registrado y si la protección específica está en modo monitoreo, el header HTTP de la respuesta del servidor.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
M	**CONSOLA DE GESTIÓN**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		
1	La consola de gestión debe ser del tipo fisico (appliance dedicado)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	IG_APSoluteVision-4-83.pdf Pág. 39, Installing APSolute Vision Physical Appliance	Verificado
2	La consola de gestión debe soportar la administración y monitoreo de los equipos que hacen parte de la propuesta. Es decir se debe administrar en balanceador físico, sus intanacias virtuales y los modulos de WAF de cada instancia virtual.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	APSVision_4-83_UG.pdf Pág. 40, What is APSolute Vision?	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

3	La consola de gestión permitirá asignar roles de administración y monitoreo de seguridad por cada uno de los equipos administrados.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	APSVision_4-83_UG.pdf Pág. 43, User Management and Role-based Access Control (RBAC)	Verificado
4	La consola de gestión debe permitir el acceso a la interfaz gráfica a través del protocolo HTTPS.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	APSVision_4-83_UG.pdf Pág. 43, APSolute Vision Platform Management	Verificado
5	La consola de gestión debe soporta autenticación remota a través de los protocolos de autenticación RADIUS, LDAP y TACACS+.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	APSVision_4-83_UG.pdf Pág. 43, User Management and Role-based Access Control (RBAC)	Verificado
6	La consola de gestión debe permitir la configuración de NTP.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	APSVision_4-83_UG.pdf Pág. 859, System NTP Commands	Verificado
7	La consola de gestión deberá permitir el acceso por REST API. Todas las operaciones que puedan realizarse a través de esta API deben estar completamente documentadas.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	APSVision_4-83_UG.pdf Pág.41, REST API support	Verificado
8	La consola de gestión deberá permitir contar con un repositorio de logs que permitan visualizar todos los cambios de configuración que se	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	APSVision_4-83_UG.pdf Pág.893, APPENDIX B – APSOLUTE VISION LOG MESSAGES AND ALERTS	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	realizan sobre los equipos.			
9	La consola de gestión debe soportar al menos las siguientes alertas de auditoria y sistema:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	APSVision_4-83_UG.pdf Pág.43, Auditing and Alerts	Verificado
	- Alarmas de servidor.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Alarmas generales del dispositivo (fan, CPU)	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Mensajes de auditoría	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
10	La consola de gestión debe permitir configuración de alertas a servidores de syslog y snmp externos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	APSVision_4-83_UG.pdf Pág.43, Auditing and Alerts	Verificado
11	La consola de gestión debe permitir sincronización con un servidor NTP	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	APSVision_4-83_UG.pdf Pág.43, Auditing and Alerts	Verificado
12	La consola de gestión debe permitir visualizar la utilización de CPU de	**ENTERADOS, ACEPTAMOS Y**	APSVision_4-83_UG.pdf Pág.337-345, Monitoring Alteon with the Dashboard	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	los dispositivos administrados	**CUMPLIMOS**		
13	La consola de gestión debe permitir creación de tareas calendarizadas para las actualizaciones de seguridad del dispositivo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	APSVision_4-83_UG.pdf Pág.304-307, CHAPTER 8 – SCHEDULING APSOLUTE VISION AND DEVICE TASKS	Verificado
14	Desde la consola de gestión se podrá realizar la actualización de la versión principal de los equipos administrados	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	APSVision_4-83_UG.pdf Pág.304-307, CHAPTER 8 – SCHEDULING APSOLUTE VISION AND DEVICE TASKS	Verificado
N	**ALERTAS Y REPORTES**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		
1	La consola de gestión debe permir generar reportes históricos de los ataques detectados y mitigados por la solución	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 27, APSolute Vision Analytics—Overview	Verificado
2	La consola de gestión debe permitir programar tareas de reportes y enviar los reportes vía correo electrónico.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 141, 12. In the Share step, do the following	Verificado
3	La consola de gestión debe permitir configurar un rango de tiempo de hasta 1 año para la generación de reportes históricos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 139, Creating a Forensics View in AVA AMS for AppWall	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

4	Debe soportar formatos PDF, CSV y HTML para los reportes históricos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 141, 11. In the Format step	Verificado
5	Debe permitir la personalización del logo de la entidad en los reportes	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 69, 5. If you require a custom logo for the Report	Verificado
6	Debe permitir escoger la o las aplicaciones que harán parte del reporte	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 139-141	Verificado
7	La consola de gestión debe permitir busquedas de eventos de seguridad a través de la definición de criterios de busqueda. Como mínimo se deben incluir los siguientes críterios:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 139-141	Verificado
	- Nombre del Ataque	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- IP Origen e IP Destino	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Nombre de la aplicación	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	- Severidad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
	- Tipo de amenaza	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
8	La consola de gestión debe permitir anidar múltiples críterios a través de expresiones regulares	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 139-141	Verificado
9	Desde la consola de gestión se deben enviar alertas de ataques	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 139-141	Verificado
10	Debe permitir escoger las aplicaciones específicas sobre los cuales se realizará la configuración de la alerta	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 139-141	Verificado
11	Desde la consola de gestión se podrá personalizar el tipo de alertas que se enviarán a través de la creación de expresiones regulares con al menos los siguientes criterios:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	APSVision_4-83_UG.pdf Pág. 595, Table 443: Packet Capture Filter Regular Expression Parameters	Verificado
	- Nombre del Ataque	**ENTERADOS, ACEPTAMOS Y**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		
	- IP Origen e IP Destino	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Nombre de la aplicación	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Severidad	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
	- Tipo de amenaza	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
12	Desde la consola de gestión se podrá configurar la severidad de la alerta	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**	APSVision_4-83_UG.pdf Pág. 128, Severity	Verificado
O	**MONITOREO Y REPORTES DE LAS APLICACIÓN BALANCEADAS**	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		
1	La consola de gestión centralizada debe contar con dashboards que resuman el estado de	**ENTERA DOS, ACEPTA MOS Y**	AVA_4-83_UG.pdf Pág. 35, Using the AVA ADC Application Dashboard	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	las aplicaciones balanceadas.	**CUMPLIMOS**		
2	Los dashboards deben entregar información de todos los balanceadores, incluyendo como mínimo: Nombre del dispositivo, estado de salud del equipo, IP de administración, factor de forma, versión, throughput, Conexiones por segundo, Conexiones por Segundo SSL y uso de CPU y memoria.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 38-44	Verificado
3	Los dashboards debe contar con un monitoreo de todos los chequeos de salud configurandos en los balanceadores.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
4	Los dashboards debe entregar al menos los siguientes valores totales de tráfico hacia las aplicaciones balanceadas: Throughput, Conexiones por Segundo y Conexiones Concurrentes	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
5	Los dashboards debe mostrar el top de aplicaciones por Throughput y por Request por segundo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

6	Los dashboards debe mostrar información de Throughput, Conexiones por Segundo, Conexiones concurrentes, Request por segundo para cada aplicación por separado.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
7	Los dashboards debe mostrar información de Throughput, Conexiones por Segundo, Conexiones concurrentes para cada servidor real que hace parte de un grupo de balanceo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
8	Los dashboards debe mostrar por cada aplicación balanceada el round trip time total, el round trip time entre el cliente y el balanceador, el round trip time entre el balanceador y la aplicación y el tiempo de respuesta de la aplicación.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
9	Para el tráfico SSL los dashboards deben mostrar las conexiones por segundo por cada aplicación, de acuerdo a la versión de TLS utilizada	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
10	Para el tráfico SSL los dashboards deben mostrar los algoritmos de intercambio de llaves por cada aplicación	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

11	Para el tráfico SSL los dashboards deben mostrar el TOP de los Ciphers utilizados por cada aplicación	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
12	Para el tráfico SSL los dashboards deben mostrar el porcentaje de handshakes rechazados por cada aplicación	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
13	Para el tráfico SSL los dashboards deben mostrar las conexiones por segundo SSL dando estadísticas gráficas de las nuevas conexiones, las conexiones reusadas y aquellas rechazadas	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
14	La consola de gestión debe incluir los logs de las transacciones que van a los sitios web públicados en en los balanceadores.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 45-52, Traffic Log Dashboard	Verificado
15	La consola de gestión debe almacenar hasta 3 meses de logs de transacciones que van a los sitios web públicados en en los balanceadores.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 45-56, Traffic Log Dashboard	Verificado
16	La consola de gestión debe permitir la navegación sobre los logs de transacciones, con al menos las siguientes características:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

17	Modificar el rango de tiempo de busqueda	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
18	Debe dar el número total de transacciones en un rango de tiempo seleccionado	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
19	Debe clasificar las conexiones en transacciones normales y transacciones fallidas, mostrando el numero total para cada una de ellas	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
20	Por cada transacción debe entregar detalles del request, el response, el tiempo de respuesta, los parámetros del cliente que realiza la conexión, detalles de SSL y los detalles del balanceo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
21	Debe permitir busquedas rápidas dentro de conjunto de logs transaccionales guardados, a través de criterios flexibles y pesonalizables.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
22	La consola de gestión debe permir generar reportes históricos de las aplicaciones balanceadas	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
23	La consola de gestión debe permitir programar tareas de reportes y enviar los	**ENTERADOS, ACEPTAMOS Y**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	reportes vía correo electrónico.	**CUMPLIMOS**		
24	La consola de gestión debe permitir configurar un rango de tiempo de hasta 1 año para la generación de reportes históricos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
25	Debe soportar formatos PDF, CSV y HTML para los reportes históricos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
26	Debe permitir la personalización del logo de la entidad en los reportes	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
27	Debe permitir escoger las aplicaciones específicas sobre los cuales se ejecutará el reporte	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
28	La consola de gestión debe permitir personalizar el contenido de los reportes con mínimo las siguientes estadísticas:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 124, Using AVA AMS Reports	Verificado
29	Tiempo de Respuesta	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

30	Throughput	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
31	Conexiones Concurrentes	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
32	Conexiones por Segundo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
33	Request por Segundo	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
P	**MONITOREO Y REPORTES DE SEGURIDAD WEB**	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		
1	La consola de gestión debe contar con un dashboard que resuma los eventos de seguridad.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág. 73, CHAPTER 3 – USING AVA AMS MODULES	Verificado
2	El dashboard debe permitir seleccionar la información a mostrar, las aplicaciones y el rango de tiempo.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág.123, Using the AppWall Dashboard	Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

3	El dashboard debe contener al menos los siguientes cuadros de información:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
4	Top de Ataques por categoría	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
5	Top de Origenes y Destinos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
6	Ataques por acción	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**	AVA_4-83_UG.pdf Pág.123-135, Using the AppWall Dashboard	Verificado
7	Top de Ataques por Severidad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
8	Geolocalización de los ataques	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
9	La consola de gestión debe permir generar reportes históricos de los ataques detectados y mitigados por la solución	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

10	La consola de gestión debe permitir programar tareas de reportes y enviar los reportes vía correo electrónico.	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
11	La consola de gestión debe permitir configurar un rango de tiempo de hasta 1 año para la generación de reportes históricos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
12	Debe soportar formatos PDF, CSV y HTML para los reportes históricos	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
13	Debe permitir la personalización del logo de la entidad en los reportes	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
14	Debe permitir escoger la o las aplicaciones que harán parte del reporte	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
15	La consola de gestión debe permitir busquedas de eventos de seguridad a través de la definición de criterios de busqueda. Como mínimo se deben incluir los siguientes críterios:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
16	Nombre del Ataque	**ENTERADOS, ACEPTAMOS Y**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

		CUMPLI MOS		
17	IP Origen e IP Destino	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
18	Nombre de la aplicación	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
19	Severidad	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
20	Tipo de amenaza	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
21	La consola de gestión debe permitir anidar múltiples críterios a través de expresiones regulares	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
22	Desde la consola de gestión se deben enviar alertas de ataques	**ENTERA DOS, ACEPTA MOS Y CUMPLI MOS**		Verificado
23	Debe permitir escoger las aplicaciones específicas sobre los cuales se realizará la	**ENTERA DOS, ACEPTA MOS Y**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	configuración de la alerta	**CUMPLIMOS**		
24	Desde la consola de gestión se podrá personalizar el tipo de alertas que se enviarán a través de la creación de expresiones regulares con al menos los siguientes criterios:	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
25	Nombre del Ataque	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
26	IP Origen e IP Destino	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
27	Nombre de la aplicación	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
28	Severidad	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado
29	Tipo de amenaza	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

30	Desde la consola de gestión se podrá configurar la severidad de la alerta	**ENTERADOS, ACEPTAMOS Y CUMPLIMOS**		Verificado

ITEM	**OTROS REQUERIMIENTOS HABILITANTES**	**CUMPLE (SI)**	**¿COMO SE VERIFICA?**	**VERIFICACION EN DOCUMENTO**
A	**OTRAS OBLIGACIONES DEL CONTRATISTA**			**FOLIO/NA**
1	Realizar Instalación, afinamiento, configuración, pruebas y puesta en funcionamiento, cuando aplique, de los equipos y software suministrado tipo APPLIANCE-FIREWALL (hardware y software) que adquiera la Universidad.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento el cumplimiento Realizar Instalación, afinamiento, configuración, pruebas y puesta en funcionamiento, cuando aplique, de los equipos y software suministrado tipo APPLIANCE-FIREWALL (hardware y software) que adquiera la Universidad.	N/A
2	Realizar las nuevas configuraciones después de realizar el proceso de Instalación y actualización, se acordará el proceso de administración de cambios para la creación de nuevas reglas o configuraciones, previa aprobación de la UNIVERSIDAD PEDAGOGICA NACIONAL.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento realizar las nuevas configuraciones después de realizar el proceso de Instalación y actualización, se acordará el proceso de administración de cambios para la creación de nuevas reglas o configuraciones, previa aprobación de la UNIVERSIDAD PEDAGOGICA NACIONAL.	N/A
3	Instalación, Transferencia de conocimientos, capacitación, visitas proactivas Mensuales, Soporte telefónico Web y en sitio cuando se solicite, Durante la vigencia del contrato, 7x24. Incluye servicio de Monitoreo.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento, Instalación, Transferencia de conocimientos, capacitación, visitas proactivas Mensuales, Soporte telefónico Web y en sitio cuando se solicite, Durante la vigencia del	N/A

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			contrato, 7x24. Incluye servicio de Monitoreo.	
4	Realizar la Actualización de nuevas versiones de software y parches, previa autorización de la UNIVERSIDAD PEDAGOGICA NACIONAL y por medio del proceso de control de cambios, Durante la vigencia de las licencias.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Realizar la Actualización de nuevas versiones de software y parches, previa autorización de la UNIVERSIDAD PEDAGOGICA NACIONAL y por medio del proceso de control de cambios, Durante la vigencia de las licencias.	N/A
6	Realizar Backup de las configuraciones antes y después de cada cambio, con el fin de garantizar una respuesta oportuna en caso de alguna eventualidad que requiera la reconfiguración de los equipos utilizados en la solución.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Realizar Backup de las configuraciones antes y después de cada cambio, con el fin de garantizar una respuesta oportuna en caso de alguna eventualidad que requiera la reconfiguración de los equipos utilizados en la solución	N/A
7	Aplicar las mejores prácticas sugeridas por el fabricante y aseguramiento de los servicios para minimizar los riesgos	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento, Aplicar las mejores prácticas sugeridas por el fabricante y aseguramiento de los servicios para minimizar los riesgos	N/A
8	El proponente deberá entregar la documentación técnica detallada de toda la actualización realizada	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El proponente deberá entregar la documentación técnica detallada de toda la actualización realizada	N/A
9	El proponente deberá entregar un informe técnico mensual durante el tiempo de garantía y/o soporte, del desempeño de la Plataforma Adquirida	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El proponente deberá entregar un informe técnico mensual durante el tiempo de garantía y/o soporte, del desempeño de la Plataforma Adquirida	N/A

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

10	Deberá realizar análisis previo de la plataforma tecnológica actual: hardware, software, red de comunicaciones, condiciones ambientales y sistemas de información.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Deberá realizar análisis previo de la plataforma tecnológica actual: hardware, software, red de comunicaciones, condiciones ambientales y sistemas de información.	N/A
11	Deberá efectuar Transferencia de conocimientos en los productos ofrecidos. Esta transferencia debe ser realizada virtual o en sitio, por una entidad certificada por el fabricante. Se debe adjuntar certificación dirigida a la Universidad Pedagógica emitida por el fabricante de dicha entidad.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Deberá efectuar Transferencia de conocimientos en los productos ofrecidos. Esta transferencia debe ser realizada virtual o en sitio, por una entidad certificada por el fabricante. Se debe adjuntar certificación dirigida a la Universidad Pedagógica emitida por el fabricante de dicha entidad.	N/A
12	Realizar las Pruebas necesarias Para garantizar el buen funcionamiento de la solución	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Realizar las Pruebas necesarias Para garantizar el buen funcionamiento de la solución	N/A
13	Efectuar administración, Seguimiento, monitoreo a los equipos objeto del contrato.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Efectuar administración, Seguimiento, monitoreo a los equipos objeto del contrato.	N/A
B	**VISITAS, INCIDENCIAS DE MANTENIMIENTO, SOPORTE Y GARANTIA**			
1	Para la prestación del servicio se requiere que el proponente cuente con un esquema de mesa de Ayuda, donde se puedan generar los reportes de incidentes frente a la prestación del servicio.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Para la prestación del servicio se requiere que el proponente cuente con un esquema de mesa de Ayuda, donde se puedan generar los reportes de incidentes frente a la prestación del servicio.	N/A
2	Adjuntar la metodología utilizada y licencia o certificación del software utilizado para la Mesa de	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Adjuntar la metodología utilizada y licencia o certificación del software	340

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	ayuda el cual sigue las mejores prácticas de ITIL		utilizado para la Mesa de ayuda el cual sigue las mejores prácticas de ITIL	
3	Detectar y reaccionar oportunamente ante incidentes de seguridad de la información, de acuerdo a los de servicio (SLAs) expuestos	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Detectar y reaccionar oportunamente ante incidentes de seguridad de la información, de acuerdo a los de servicio (SLAs) expuestos	N/A
4	Brindar constantemente recomendaciones que permitan obtener un mejor nivel de mitigación de riesgos derivados del uso de la tecnología	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Brindar constantemente recomendaciones que permitan obtener un mejor nivel de mitigación de riesgos derivados del uso de la tecnología	N/A
5	Se debe brindar un componente de alarma para la detección automática de eventos de seguridad, que faciliten la gestión de los mismos sobre la infraestructura tecnológica	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Se debe brindar un componente de alarma para la detección automática de eventos de seguridad, que faciliten la gestión de los mismos sobre la infraestructura tecnológica	N/A
6	En caso de no ser posible la solución remota o telefónica, se requiere prestación del servicio en sitio, de acuerdo a los niveles de servicios pactados	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento En caso de no ser posible la solución remota o telefónica, se requiere prestación del servicio en sitio, de acuerdo a los niveles de servicios pactados	N/A
7	Una vez realizada la instalación, puesta en marcha del producto y soportada la estabilidad de la solución, durante la vigencia de las Licencias deberá realizar una visita mensual para validar el correcto funcionamiento de la solución.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Una vez realizada la instalación, puesta en marcha del producto y soportada la estabilidad de la solución, durante la vigencia de las Licencias deberá realizar una visita mensual para validar el correcto funcionamiento de la solución.	N/A

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

8	Se requiere servicio de análisis de log y generación de reportes de manera periódica.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Se requiere servicio de análisis de log y generación de reportes de manera periódica.	N/A
9	El contratista deberá brindar soporte remoto y/o en sitio dependiendo el nivel de criticidad de la solicitud realizada para fallas e implementaciones.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El contratista deberá brindar soporte remoto y/o en sitio dependiendo el nivel de criticidad de la solicitud realizada para fallas e implementaciones.	N/A
10	Para el presente proceso el contratista debe colocar un gerente de proyectos. Ingeniero con Especialización en seguridad de la información. Experiencia como Auditor líder en la norma ISO27001 ver 2013, CISM (Certified Information Security Manager. Para lo cual deberá presentar Hoja de vida documentada, soportada y tarjeta profesional. Experiencia demostrable desarrollando proyectos de temas de sistemas de seguridad de la información. Adjuntar mínimo tres (3) certificaciones de su participación en dichos proyectos como gerente y/o consultor en procesos de seguridad informática.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento ara el presente proceso el contratista debe colocar un gerente de proyectos. Ingeniero con Especialización en seguridad de la información. Experiencia como Auditor líder en la norma ISO27001 ver 2013, CISM (Certified Information Security Manager. Para lo cual deberá presentar Hoja de vida documentada, soportada y tarjeta profesional. Experiencia demostrable desarrollando proyectos de temas de sistemas de seguridad de la información. Adjuntar mínimo tres (3) certificaciones de su participación en dichos proyectos como gerente y/o consultor en procesos de seguridad informática.	243
11	Realizar y presentar un (1) informe de vulnerabilidades que incluya lista de vulnerabilidades encontradas con su respectivo plan de remediación y efectuar la presentación y socialización al personal técnico de la Subdirección de Gestión de Sistemas de Información. Lo	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Realizar y presentar un (1) informe de vulnerabilidades que incluya lista de vulnerabilidades encontradas con su respectivo plan de remediación y efectuar la presentación y socialización al personal técnico de la Subdirección de Gestión de	N/A

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	anterior, dentro del marco de la Norma ISO-27000.		Sistemas de Información. Lo anterior, dentro del marco de la Norma ISO-27000.	
12	El proponente deberá adjuntar a la propuesta mínimo una certificación de haber realizado un análisis de vulnerabilidad en una entidad superior a 500 usuarios y otra certificación adicional en una entidad de 3000 usuarios.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El proponente deberá adjuntar a la propuesta mínimo una certificación de haber realizado un análisis de vulnerabilidad en una entidad superior a 500 usuarios y otra certificación adicional en una entidad de 3000 usuarios.	257, 258
13	El ingeniero que realizará el análisis de vulnerabilidad debe adjuntar mínimo 2 certificaciones de experiencia en mínimo 2 entidades en donde haya realizado, soportado consecutivamente durante 5 años esta labor de análisis de vulnerabilidades.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El ingeniero que realizará el análisis de vulnerabilidad debe adjuntar mínimo 2 certificaciones de experiencia en mínimo 2 entidades en donde haya realizado, soportado consecutivamente durante 5 años esta labor de análisis de vulnerabilidades.	259
14	Entregar un documento de continuidad de la operación de la Universidad en caso de fallas de seguridad, dentro del marco de la Norma ISO-22301.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Entregar un documento de continuidad de la operación de la Universidad en caso de fallas de seguridad, dentro del marco de la Norma ISO-22301.	N/A

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

15	El proponente debe ser distribuidor autorizado del fabricante del equipo ofertado, lo cual debe acreditar, mediante presentación de certificación vigente, expedida por el representante en Colombia, no mayor a 15 días anteriores a la fecha del cierre de la presente Convocatoria Pública y dirigida a la UNIVERSIDAD PEDAGOGICA NACIONAL, donde se especifique se encuentra autorizado para vender y soportar técnicamente las soluciones de seguridad en Colombia.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El proponente debe ser distribuidor autorizado del fabricante del equipo ofertado, lo cual debe acreditar, mediante presentación de certificación vigente, expedida por el representante en Colombia, no mayor a 15 días anteriores a la fecha del cierre de la presente Convocatoria Pública y dirigida a la UNIVERSIDAD PEDAGOGICA NACIONAL, donde se especifique se encuentra autorizado para vender y soportar técnicamente las soluciones de seguridad en Colombia.	286
16	La garantía de todos los equipos y productos suministrado debe ser mínimo (1) Un año, a partir de la fecha de la aprobación de la póliza.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento La garantía de todos los equipos y productos suministrado debe ser mínimo (1) Un año, a partir de la fecha de la aprobación de la póliza.	N/A
17	El oferente deberá realizar el correspondiente soporte técnico en sitio (7x24) cada vez que se realice el requerimiento por fallas de funcionamiento del producto durante el tiempo de vigencia del contrato y de las licencias.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El oferente deberá realizar el correspondiente soporte técnico en sitio (7x24) cada vez que se realice el requerimiento por fallas de funcionamiento del producto durante el tiempo de vigencia del contrato y de las licencias.	N/A
18	El soporte deberá incluir la puesta en marcha de últimas versiones y actualizaciones necesarias para corregir problemas y efectuar mejoras sobre la solución y mantenerla actualizada en su última versión disponible en el mercado.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El soporte deberá incluir la puesta en marcha de últimas versiones y actualizaciones necesarias para corregir problemas y efectuar mejoras sobre la solución y mantenerla actualizada en su última versión disponible en el mercado.	N/A

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

19	El oferente debe ofrecer soporte técnico vía telefónica e Internet, como primer nivel de atención.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El oferente debe ofrecer soporte técnico vía telefónica e Internet, como primer nivel de atención.	N/A
20	El oferente debe realizar la Generación y envío de reportes mensuales del estado de la solución implementada durante la duración del contrato	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El oferente debe realizar la Generación y envío de reportes mensuales del estado de la solución implementada durante la duración del contrato	N/A
21	El proponente debe especificar claramente en su propuesta los datos mediante los cuales la UNIVERSIDAD PEDAGOGICA NACIONAL podrá solicitar los servicios de soporte y que deberán ser como mínimo: Una dirección de correo electrónico, un sistema de tickets vía web, un teléfono fijo y por lo menos una línea de celular, ésta última disponible 7 días x 24 horas a la semana. Durante la vigencia de las licencias, el proponente debe realizar dos (2) mantenimientos preventivos de la solución, para ello debe entregar un plan de trabajo que contenga al menos: Nombre de la actividad, tiempo estimado, fecha estimada, posibles afectaciones y responsables. Así mismo, al finalizar el mantenimiento preventivo debe entregar un informe con los resultados de éste.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El proponente debe especificar claramente en su propuesta los datos mediante los cuales la UNIVERSIDAD PEDAGOGICA NACIONAL podrá solicitar los servicios de soporte y que deberán ser como mínimo: Una dirección de correo electrónico, un sistema de tickets vía web, un teléfono fijo y por lo menos una línea de celular, ésta última disponible 7 días x 24 horas a la semana. Durante la vigencia de las licencias, el proponente debe realizar dos (2) mantenimientos preventivos de la solución, para ello debe entregar un plan de trabajo que contenga al menos: Nombre de la actividad, tiempo estimado, fecha estimada, posibles afectaciones y responsables. Así mismo, al finalizar el mantenimiento preventivo debe entregar un informe con los resultados de éste.	288

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

22	La garantía ofrecida por el fabricante debe cubrir todos los incidentes por fallas de Hardware y Software. Si la falla no puede ser resuelta por el fabricante dentro de las 12 horas siguientes al reporte del incidente (Interrupción del servicio altamente critica para la Universidad Pedagógica), el proponente se debe comprometer a gestionar con el fabricante, el cambio del equipo de las mismas o mejores condiciones técnicas, y a restablecer el servicio en un periodo adicional de máximo de 24 horas.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento La garantía ofrecida por el fabricante debe cubrir todos los incidentes por fallas de Hardware y Software. Si la falla no puede ser resuelta por el fabricante dentro de las 12 horas siguientes al reporte del incidente (Interrupción del servicio altamente critica para la Universidad Pedagógica), el proponente se debe comprometer a gestionar con el fabricante, el cambio del equipo de las mismas o mejores condiciones técnicas, y a restablecer el servicio en un periodo adicional de máximo de 24 horas.	N/A
23	El proponente deberá demostrar que cuenta con unos equipos Firewall Appliances del mismo fabricante de los equipos ofertados, que permitirán reemplazar los equipos que adquiera la Universidad en caso de alguna falla o indisponibilidad de los mismos.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El proponente deberá demostrar que cuenta con unos equipos Firewall Appliances del mismo fabricante de los equipos ofertados, que permitirán reemplazar los equipos que adquiera la Universidad en caso de alguna falla o indisponibilidad de los mismos.	292
C	**OTRAS CERTIFICACIONES Y CAPACITACIÓN DEL SISTEMA**			
1	De acuerdo con lo establecido en el Artículo 5 de la resolución 2710 de 2017 del Ministerio de las Tecnologías de Información y Comunicaciones, el proponente deberá entregar certificación del fabricante en donde se evidencie que la solución ofertada soporta IPV6 nativo en coexistencia con IPV4, de la solución o servicios listados en las	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento De acuerdo con lo establecido en el Artículo 5 de la resolución 2710 de 2017 del Ministerio de las Tecnologías de Información y Comunicaciones, el proponente deberá entregar certificación del fabricante en donde se evidencie que la solución ofertada soporta IPV6 nativo en coexistencia	286

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	especificaciones técnicas mínimas, expedida por el fabricante.		con IPV4, de la solución o servicios listados en las especificaciones técnicas mínimas, expedida por el fabricante.	
2	Los proponentes deben adjuntar certificaciones vigentes del fabricante dirigidas a la Universidad que incluya los siguientes aspectos:	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Los proponentes deben adjuntar certificaciones vigentes del fabricante dirigidas a la Universidad que incluya los siguientes aspectos:	286
3	Carta expedida por el fabricante con autorización al distribuidor para vender lo requerido, dirigida a la Universidad Pedagógica Nacional, con fecha de expedición no mayor a quince (15) días antes del cierre de la presente convocatoria.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Carta expedida por el fabricante con autorización al distribuidor para vender lo requerido, dirigida a la Universidad Pedagógica Nacional, con fecha de expedición no mayor a quince (15) días antes del cierre de la presente convocatoria.	286
4	Indicando que son aptos para el diseño en implementación, instalación y puesta en producción de la solución tecnológica ofrecida	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Indicando que son aptos para el diseño en implementación, instalación y puesta en producción de la solución tecnológica ofrecida	286
5	El proponente debe haber renovado, licenciado, instalado o configurado mínimo 3 soluciones de características similares del mismo fabricante de Firewall de la solución ofertada en alta Disponibilidad. Adjuntar Certificaciones en donde se describa: la Entidad, que expide la certificación, Objeto, Tiempo de ejecución, nombre, teléfono de quien firma la certificación.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El proponente debe haber renovado, licenciado, instalado o configurado mínimo 3 soluciones de características similares del mismo fabricante de Firewall de la solución ofertada en alta Disponibilidad. Adjuntar Certificaciones en donde se describa: la Entidad, que expide la certificación, Objeto, Tiempo de ejecución,	235

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

			nombre, teléfono de quien firma la certificación.	
6	Se verificará la experiencia del proponente en la celebración y ejecución de máximo de tres (3) contratos cuyo objeto corresponda o esté relacionado con el de ésta convocatoria, ejecutados en los últimos 4 años anteriores a la fecha del cierre del presente proceso de selección cuya sumatoria sea igual o superior al 100% del presupuesto oficial representado en SMMLV. Dos (2) certificaciones de Entidades Educativas Públicas y Una (1) certificación de una Entidad del Sector Público.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Se verificará la experiencia del proponente en la celebración y ejecución de máximo de tres (3) contratos cuyo objeto corresponda o esté relacionado con el de ésta convocatoria, ejecutados en los últimos 4 años anteriores a la fecha del cierre del presente proceso de selección cuya sumatoria sea igual o superior al 100% del presupuesto oficial representado en SMMLV. Dos (2) certificaciones de Entidades Educativas Públicas y Una (1) certificación de una Entidad del Sector Público.	235
7	El proponente deberá capacitar mínimo 1 persona directamente con la marca de los equipos Firewall Ofrecidos. Se debe entregar igual número de Voucher para presentación exámenes de certificación.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El proponente deberá capacitar mínimo 1 persona directamente con la marca de los equipos Firewall Ofrecidos. Se debe entregar igual número de Voucher para presentación exámenes de certificación.	N/A
8	El proponente debe brindar capacitación de la solución instalada cuando la Universidad lo solicite. (mínimo una capacitación semestral).	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El proponente debe brindar capacitación de la solución instalada cuando la Universidad lo solicite. (mínimo una capacitación semestral).	N/A

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

9	El proponente debe entregar en físico y en digital la documentación de la configuración del estado inicial y del estado posterior a la implementación de la solución.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El proponente debe entregar en físico y en digital la documentación de la configuración del estado inicial y del estado posterior a la implementación de la solución.	N/A
10	El proponente debe garantizar la capacitación y certificación de la solución ofrecida.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El proponente debe garantizar la capacitación y certificación de la solución ofrecida.	N/A
11	El proponente debe contar como mínimo con dos (2) Ingenieros Certificados por el fabricante como expertos de la solución Firewall ofrecida. Adjuntar (Hoja de vida, certificaciones del fabricante, Parafiscales).	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El proponente debe contar como mínimo con dos (2) Ingenieros Certificados por el fabricante como expertos de la solución Firewall ofrecida. Adjuntar (Hoja de vida, certificaciones del fabricante, Parafiscales).	135, 294, 303
12	La implementación de la solución Web Aplication Firewall debe hacerse directamente por parte del fabricante. Para lo cual debe contar con mínimo 2 ingenieros en Colombia con las siguientes certificaciones:	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento La implementación de la solución Web Aplication Firewall debe hacerse directamente por parte del fabricante. Para lo cual debe contar con mínimo 2 ingenieros en Colombia con las siguientes certificaciones: adjunto HV	325
13	Primer ingeniero. Certified information systems security professional , Ec-council certified ethical hacker. Certified Security Expert, Certified Security Administrator de la solución Firewall ofrecida y Certified Security Specialist, Certified Application Specialist de la solución Web Aplication Firewall ofrecida.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Primer ingeniero. Certified information systems security professional , Ec-council certified ethical hacker. Certified Security Expert, Certified Security Administrator de la solución Firewall ofrecida y Certified Security Specialist, Certified Application Specialist de la solución Web Aplication Firewall ofrecida. Adjunto HV	319 (El Proponente cumple con lo exigido en la adenda No. 1)

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

14	El segundo Ingeniero Certified porfessional Services Enginer (de la solución Web Aplication Firewall ofrecida.)	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El segundo Ingeniero Certified porfessional Services Enginer (de la solución Web Aplication Firewall ofrecida.) Adjunto HV	325 (El Proponente cumple con lo exigido en la adenda No. 1)
D	**CERTIFICACIONES DEL GRUPO DE TRABAJO DEL PROPONENTE**			
1	Un Ingeniero especialista en Proyectos Informáticos Certificado por el PMI como PMP, que actuará como Gerente y/o Líder del Proyecto.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento Un Ingeniero especialista en Proyectos Informáticos Certificado por el PMI como PMP, que actuará como Gerente y/o Líder del Proyecto. Adjunto HV	358
2	El Auditor del análisis de vulnerabilidades deberá ser certificado ISO 27001 y Ethical Hacking. Deberá aportar certificación de experiencia laboral del empleador contratante y/o representante del proveedor o fabricante donde conste haber dirigido al menos un equipo de auditores como auditor líder en ISO27001.	SI CUMPLIMOS	Certificamos bajo la gravedad de juramento El Auditor del análisis de vulnerabilidades deberá ser certificado ISO 27001 y Ethical Hacking. Deberá aportar certificación de experiencia laboral del empleador contratante y/o representante del proveedor o fabricante donde conste haber dirigido al menos un equipo de auditores como auditor líder en ISO27001. Adjunto HV	346 (El Proponente cumple con lo exigido en la adenda No. 1)

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

Resultado de la verificación de requerimientos en el numeral 3.2. REFERENTES Y CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS:

Teniendo en cuenta que el proponente **SE COMPROMETE A CUMPLIR** con todas y cada una de las especificaciones técnicas contenidas en este numeral y en el pliego de condiciones, el resultado de la verificación es que el proponente **CUMPLE.**

EMPRESA	VERIFICACIÓN DEL NUMERAL 3.2 REFERENTES Y CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS	SE VERIFICA EN FOLIOS DESDE - HASTA
SOFTSECURITY S.A.S	**CUMPLE**	**10 – 118**

b) VERIFICACIÓN DE LA EXPERIENCIA DEL PROPONENTE

Los términos de referencia de la CONVOCATORIA PUBLICA No. 5 DE 2021 dicen lo siguiente:

Experiencia (FORMATO No.7).

Se verificará la experiencia del proponente en la celebración y ejecución de máximo tres (3) contratos cuyo objeto corresponda o esté relacionado con el de esta convocatoria, ejecutados en los últimos 4 años anteriores a la fecha del cierre del presente proceso de selección cuya sumatoria sea igual o superior al 100% del presupuesto oficial representado en SMMLV. Además, el respectivo contrato, deberá contemplar todos los códigos del Clasificador de Bienes y Servicios (UNSPSC) en el tercer nivel, que se relacionan a continuación:

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

CODIGOS UNSPSC	CLASE
43233200	SOFTWARE DE SEGURIDAD Y PROTECCIÓN
43222500	EQUIPO DE SEGURIDAD DE RED
43222600	EQUIPO DE SERVICIO DE RED

REGLAS PARA LA VALORACIÓN DE LA EXPERIENCIA DE CONSORCIOS, UNIONES TEMPORALES O PROMESA DE SOCIEDAD FUTURA:

Los proponentes plurales deberán tenerse en cuenta los siguientes criterios:

Regla de Proporcionalidad: Cuando la propuesta se presente en consorcio o unión temporal, o promesa de sociedad futura, deberá acreditar la experiencia de acuerdo con el porcentaje de participación en la figura asociativa (expresada en SMLMV).

NOTA 1: El proponente plural debe cumplir con el 100% de los requisitos exigidos en la experiencia del proponente, es decir es obligatorio que cada uno de los integrantes acredite experiencia.

JUSTIFICACIÓN DE LA REGLA DE PROPORCIONALIDAD:

Se justifica la regla de proporcionalidad establecida por la Universidad, en consideración a que todos los integrantes de una figura asociativa deberán ostentar experiencia que permita verificar la idoneidad del futuro contratista en la ejecución de proyectos con alcances similares al contratado. Lo anterior, tiene con fundamento legal responsabilidad solidaria de todas y cada una de las obligaciones derivadas de la propuesta y del contrato, consagrada en el artículo 7 de la Ley 80 de 1993.

Así mismo, conforme lo prevé el artículo 5 de la ley 1150 de 2007, la exigencia de tales condiciones debe ser adecuada y proporcional a la naturaleza del contrato a suscribir y a su valor, pues como se expresó, es necesario contar con proponentes que acrediten experticia en la ejecución de contratos como el requerido por la UPN situación que conllevó a establecer la regla de proporcionalidad, a efectos que de forma equitativa y conforme a cada figura asociativa que se cree, atendiendo a un criterio objetivo de participación los integrantes de las mismas aúnen esfuerzos y garanticen en la ejecución del contrato el conocimiento y la experticia de cualquiera de los mismos para lograr su éxito en los tiempos y las condiciones técnicas previstas.

La anterior regla tiene como sustento jurisprudencial en la posibilidad de fijar límites al número de participantes o de fijar reglas para determinar su capacidad real o material, SALA DE LO

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

CONTENCIOSO ADMINISTRATIVO, SECCIÓN TERCERA, consejera Ponente: MARÍA ELENA GIRALDO GÓMEZ, Radicación Nº 73001-23-31-000-1997-04707- 02(15188).

Nota 1: Para el caso de contratos que sean aportados por socios de empresas que no cuentan con más de tres (3) años de constituidas, en caso de ser necesario se deberá aportar adicional a los documentos válidos para la acreditación de experiencia, un documento debidamente suscrito por el representante legal y el revisor fiscal o contador público (según corresponda), donde se indique la conformación societaria de la empresa, y los respectivos contratos acreditados, los cuales deben estar inscritos en el RUP de cada socio.

LA Universidad se reserva el derecho de verificar durante la evaluación y hasta la adjudicación la información aportada por el
proponente, así como la información que reposa en la cámara de comercio u otras plataformas públicas y solicitar los soportes que considere convenientes tales como: certificaciones, copias de los contratos, facturas de venta, copia de los medios de pago, actas suscritas, actas de liquidación, estados financieros, copia de pago de impuestos o cualquier otro documento.

La verificación de esta experiencia, se efectuará de conformidad con la información relacionada en el **FORMATO No. 6**.

Resultado de la verificación de la EXPERIENCIA DEL PROPONENTE: Teniendo en cuenta que el proponente presenta certificaciones de experiencia de acuerdo a lo solicitado, el resultado de la verificación es que el proponente **CUMPLE.**

EMPRESA	EXPERIENCIA DEL PROPONENTE	SE VERIFICA EN FOLIOS DESDE - HASTA
SOFTSECURITY S.A.S	**CUMPLE**	**234 – 239**

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

c) VERIFICACIÓN DE LOS CÓDIGOS RUP - REGISTRO ÚNICO DE PROPONENTES

Los términos de referencia de la CONVOCATORIA PUBLICA No. 5 DE 2021 dicen lo siguiente:

"Se verificará la experiencia del proponente en la celebración y ejecución de máximo tres (3) contratos cuyo objeto corresponda o esté relacionado con el de esta convocatoria, ejecutados en los últimos 4 años anteriores a la fecha del cierre del presente proceso de selección cuya sumatoria sea igual o superior al 100% del presupuesto oficial representado en SMMLV. Además, el respectivo contrato, deberá contemplar todos los códigos del Clasificador de Bienes y Servicios (UNSPSC) en el tercer nivel, que se relacionan a continuación:

CODIGO UNSPSC	CLASE
43233200	SOFTWARE DE SEGURIDAD Y PROTECCIÓN
43222500	EQUIPO DE SEGURIDAD DE RED
43222600	EQUIPO DE SERVICIO DE RED

".

Resultado de la verificación de los CÓDIGOS RUP - REGISTRO ÚNICO DE PROPONENTES: Teniendo en cuenta que el proponente presenta los **CÓDIGOS RUP** de acuerdo a lo solicitado, el resultado de la verificación es que el proponente **CUMPLE.**

PROPONENTES	Código	Clase	Cumple	Se verifica en folios Desde - hasta
SOFTSECURITY S.A.S	43233200	Software de seguridad y protección	SI	**207-207**
	43222500	Equipo de seguridad de red	SI	**207-207**
	43222600	Equipo de servicio de red	SI	**207-207**

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

3. RESULTADOS DE LA EVALUACIÓN Y LA VERIFICACIÓN

EVALUACION ECONOMICA Y FACTORES PONDERABLES DE LAS PROPUESTAS HABILITADAS							
PROPONENTES	**VR. PROPUESTA ANTES DE I.V.A**	**I.V.A**	**VR. PROPUESTA DESPUES DE I.V.A**	**DIFERENCIA CONTRA PRESUPUESTO**	**FACTOR ECONOMICO (Regla de Tres Inversa)**	**FACTOR TÉCNICO - Valores agregados**	**TOTAL PUNTOS**
SOFTSECURITY S.A.S	$ 996.638.600	$ 189.361.334	$ 1.185.999.934	$ 2.167.057	400	600	1000
PRESUPUESTO	$ 1.188.166.991						

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

	VERIFICACIÓN DE CUMPLIMIENTO DE REQUISITOS DE LAS OFERTAS		
PROPONENTES	**Referentes y características técnicas mínimas requeridas Experiencia del proponente**	**Experiencia del proponente**	**Códigos Rup - registro único de proponentes**
SOFTSECURITY S.A.S	**CUMPLE**	**CUMPLE**	**CUMPLE**

4. CONCLUSIÓN

La Subdirección de Gestión de sistemas de Información, después de revisar las propuestas recibidas, realizar la verificación de los FACTORES: ECONOMICO, TECNICOS, VALORES AGREGADOS, REFERENTES Y CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS, CÓDIGOS RUP, CERTIFICACIONES DE EXPERIENCIA y la evaluación general correspondiente de acuerdo con lo estipulado en los términos de referencia, concluye que la empresa **SOFTSECURITY S.A.S** cumple desde lo económico, lo técnico, valores agregados y demás requisitos exigidos en la CONVOCATORIA PUBLICA de la referencia.

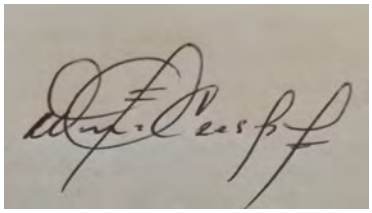
5. EQUIPO DE EVALUACIÓN TÉCNICA

Esta evaluación fue:

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co

Realizada por:

- Ing. HENDRIX SUAREZ CARDENAS



- Ing. WILLIAM RAFAEL CRESPO ARZUZA

Revisada por: 

- Ing. HENRY AUGUSTO CORDOBA SANCHEZ

Esta Evaluación Técnica se firma en Bogotá. D.C, a los 14 días del mes de diciembre de 2021

HENRY AUGUSTO CORDOBA SANCHEZ

Subdirector de Gestión de Sistemas de Información.

/Proyecto/elaboró: William R. Crespo Arzuza

Calle 72 No. 11-86
PBX: (571) 5941894 – Ext. 149
Bogotá D. C.
www.pedagogica.edu.co