UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

"*CONTRATAR LA ADQUISICIÓN, INSTALACIÓN Y PUESTA EN CORRECTO FUNCIONAMIENTO DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL COMPUESTA POR DOS EQUIPOS PARA GARANTIZAR LA ALTA DISPONIBILIDAD (HA) PARA LA UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS INCLUYENDO LICENCIAMIENTO, SOPORTE Y ACTUALIZACIONES (UPDATE Y UPGRADE).* "

MATRIZ DE EVALUACION TECNICA

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
1	Generalidades	La solución de Seguridad Perimetral (HA) debe estar compuesto por todo el hardware, software, accesorios y licenciamiento necesarios para su funcionamiento incluyendo alta disponibilidad HA.	Propuesta tecnica pagina7 punto 3 Solución Propuesta Palo Alto Networks, con un clúster en HA compuesto de 2 equipos PA-3420	CUMPLE		Se contenplan dos equipos QUANTUM FORCE 9700 para alta disponibilidad. https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 4 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
2	Generalidades	El sistema debe contar con una totalidad de dos equipos con el fin de minimizar los puntos de falla, optimizar el espacio en el data center, optimizar el uso de las conexiones de red y facilitar la administración incluyendo el sistema de monitoreo y reportes. Estos deben trabajar de forma redundante entre sí en Alta disponibilidad (HA) soportando todos los servicios que presta la solución de seguridad perimetral HA.	Propuesta tecnica pagina7 punto 3 Solución Propuesta Palo Alto Networks, con un clúster en HA compuesto de 2 equipos PA-3420	CUMPLE		Se contenplan dos equipos QUANTUM FORCE 9700 para alta disponibilidad. https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 4 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
3	Generalidades	El hardware y software que ejecuten las funcionalidades del sistema deben ser de tipo Appliance. No serán aceptados equipamientos servidores y sistema operativo de uso genérico.	Propuesta tecnica pagina7 punto 3 Solución Propuesta Palo Alto Networks, con un clúster en HA compuesto de 2 equipos PA-3420	CUMPLE		Se contenplan el modelo QUANTUM FORCE 9700 https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 3 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
4	Generalidades	Los equipos ofrecidos deben ser adecuados para montaje en rack 19". Cada equipo puede ocupar máximo 3 unidades de Rack.	El tamaño por dispositivo es de 1 U Rackstand 19" https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/es_LA/resources/datasheets/pa-3400-series	CUMPLE		https://sc1.checkpoint.com/documents/Appliances/GSG_9000/EN/CP_9000_Appliances_GettingStartedGuide.pdf pagina 37 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
5	Generalidades	El software del sistema deberá ser ofertado en la última versión estable y recomendada por el fabricante	Los equipos propuestos soportan las ultima version de PANOS disponible 11,2 https://docs.paloaltonetworks.com/compatibility-matrix/reference/supported-os-releases-by-model/palo-alto-networks-next-gen-firewalls#id9680433e-055f-4f38-a7d0-6d31e7d557bc	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_RN/CP_R81.20_ReleaseNotes.pdf Pagina: 1 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
6	Generalidades	El sistema debe tener la capacidad de identificar al usuario de red con integración a Microsoft Active Directory, Radius o LDAP sin la necesidad de instalación de agente en el Controlador de dominio, ni en las estaciones de los usuarios.	PanOS permite la identificacion de usuarios a traves de el agentless de PANOS y a traves de User ID agente instalado en un servidor quien revisara las sesiones y mapeara los usuarios https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/enable-user-id	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_IdentityAwareness_AdminGuide/CP_R81.20_IdentityAwareness_AdminGuide.pdf pagina: 36, 45, 184 y 192 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
7	Generalidades	El fabricante de la solución ofrecida por el proponente, debe pertenecer al cuadrante de líderes de Gartner para *"Enterprise Network Firewall"* o *"Firewalls de Redes Empresariales"* o líderes en la escala The Forrester WAVE™ en los últimos 3 años.	Forrester Wave™: Enterprise Firewall Solutions (Q4 2024) incluyó a Palo Alto Networks como: líderhttps://start.paloaltonetworks.com/forrester-wave-firewall-2024.html En cuanto a Gartner Palo Alto ha sido nombrado Líder durante más de diez años consecutivos en el Magic Quadrant for Network Firewalls https://start.paloaltonetworks.com/gartner-sse-mq-leader-2025	CUMPLE		Se adjuntan enlaces de market network firewall donde checkpoint es uno de los principales participatan de firewall en el mercado https://www.gartner.com/reviews/market/network-firewalls https://engage.checkpoint.com/2024-forrester-wave-enterprise-firewall-solutions-report Pagina: No aplica	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta. Sin embargo la información es encontrada en: https://start.paloaltonetworks.com/forrester-wave-firewall-2024.html
8	Generalidades	Los equipos deben estar certificados para IPv6 en Firewall por USGv6 o IPv6 Ready.	Los equipos poseen la certificacion https://www.paloaltonetworks.com/legal-notices/trust-center/usgv6	CUMPLE		Se coloca enlace del registro de ipv6 en donde indica que Check Point Software Technologies, Ltd. en los productos Check Point Security Gateway en el release R81.20 esta soportado https://www.iol.unh.edu/registry/usgv6?name=&test_suites%5BFW%5D=FW Pagina: No aplica	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta. Sin embargo la información es encontrada en: https://www.iol.unh.edu/registry/usgv6?name=&test_suites%5BFW%5D=FW
9	Generalidades	El sistema debe incluir actualización automática de firmas de prevención de intrusos (IPS), bloqueo de archivos maliciosos (Antivirus y Antispyware), Filtrado WEB por categorías e identificación de aplicaciones.	Las firmas mencionadas se pueden actualizar de manera automatica https://docs.paloaltonetworks.com/pan-os/11-2/pan-os-web-interface-help/device/device-dynamic-updates	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Topics-TPG/Threat_Prevention_Scheduled_Updates.htm en el lace adjunto se evidencia que soporta la actualizacion automatica de los servicios adquiridos. leer "Introduction to Scheduled Updates" Pagina:No aplica	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
10	Generalidades	Motor de procesamiento en paralelo: el módulo de hardware del plano de control y el módulo de hardware del plano de datos deben estar separados y deben estar embebidos en cada equipo.	La arquitectura de Palo Alto implementa un planeo dataplane separado del control plane, aprovechando su Single-Pass Parallel Processing Architecture, donde cada equipo posee módulos integrados para ambos planos en hardware dedicado https://www.paloaltonetworks.com/resources/pa-series-next-generation-firewalls-hardware-architectures PA3400 https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/single-pass-parallel-processing-architecture	CUMPLE		https://www.checkpoint.com/downloads/products/IPS_Engine_Architecture.pdf Pagina 5 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
11	Generalidades	Los equipos ofertados no se encuentran en periodo de fin de venta (end-of-life), ni en fin de venta (end-of-sale) y su ciclo de vida útil no es inferior a cinco (5) años	No se ha declarado ningun EOL o EOS para Los equipos ofertados https://www.paloaltonetworks.com/services/support/end-of-life-announcements/hardware-end-of-life-dates	CUMPLE		Check Point publica listas de productos activos y ciclos de vida. Los equipos nuevos cumplen con este requisito: https://www.checkpoint.com/support-services/support-life-cycle-policy/ por lo que se puede evidencias que lo equipos 9700 aun esta activos y no cuentan con fin de venta ni de soporte del fabricante Pagina:No aplica	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
12	Generalidades	Debe permitir el control de políticas por identificación de País.	Se permite el bloqueo por pais: https://live.paloaltonetworks.com/t5/community-blogs/geolocation-and-geoblocking/ba-p/315433	CUMPLE		https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_Quantum_SecurityGateway_Guide/Topics-FWG/Security-Policy.htm?Highlight=GEO Pagina 35 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
13	Generalidades	El proveedor debe presentar certificación expedida por la casa matriz donde se indica que es canal Partner en alguno de los niveles superiores de certificación según la marca, teniendo en cuenta que en orden ascendente los niveles de certificación son: Select, Advanced o Expert / Professional, Premier o Elite / Innovator, Platinum o Diamond / Premier, Gold o Platinum / o el equivalente a la marca.	Se adjunta certificacion	CUMPLE		Certificación Partner Autorizado Check Point pagina 385 del presente documento	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
14	Generalidades	La solución ofrecida debe tener un módulo en el sistema de seguridad o en la nube que permita enriquecer la comprensión de la implementación sobre la solución de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA) adquirida. Dentro de las características principales debe: * Evaluar la configuración del firewall e identificar áreas de mejora (políticas de seguridad). * Proporcionar un acceso fácil a los datos de telemetría históricos y en tiempo real del firewall. * Detectar problemas del sistema, estado de salud del firewall. * Contemplar la adopción de buenas prácticas en materia de configuración de los diferentes módulos de seguridad de la solución, como mínimo estos: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs.	Se realiza a traves del servicio SAAS Strata Cloud manager Essentials https://docs.paloaltonetworks.com/strata-cloud-manager/activation-and-onboarding/strata-cloud-manager-licenses-and-support	CUMPLE		https://www.checkpoint.com/es/cyber-hub/network-security/what-is-firewall/firewall-configuration/ https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_SitetoSiteVPN_AdminGuide/Content/Topics-VPNSG/Quantum-Safe-Key-Exchange.htm Pagina 326 - 334 del link https://support.checkpoint.com/results/sk/sk178566	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
15	Alta disponibilidad (HA)	Soporta configuración de alta disponibilidad (HA) en los modos Activo/Pasivo y Activo/Activo en modo transparente y en Layer 3.	Los equipos ofertados poseen la capacidad de configuracion en HA https://docs.paloaltonetworks.com/ngfw/administration/high-availability/ha-overview	CUMPLE		https://sc1.checkpoint.com/documents/SMB_R80.20.10/AdminGuides/Locally_Managed/EN/Content/Topics/Configuring-High-Availability.htm https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf Pagina 4 del link https://support.checkpoint.com/results/sk/sk162637	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
16	Alta disponibilidad (HA)	El modo HA (modo de Alta-Disponibilidad) debe permitir monitoreo de fallo de link.	https://docs.paloaltonetworks.com/ngfw/administration/high-availability/ha-overview	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SitetoSiteVPN_AdminGuide/Topics-VPNSG/Link-Selection.htm?Highlight=link%20failure%20monitoring pagina 451 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
17	Alta disponibilidad (HA)	El modo de alta disponibilidad debe contar con detección de fallas, en donde se visualice las posibles caídas y como solucionarlas.	https://docs.paloaltonetworks.com/ngfw/administration/high-availability/ha-overview	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Overview-Management-High-Availability.htm? pagina 452 455	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
18	Capacidades y cantidades	El equipo Next Generation Firewall (NGFW) debe estar en la capacidad de identificar y procesar el tráfico en su totalidad inspeccionado en capa 7 de aplicación.	Los equipos de palo alto son equipos de capa de aplicación L7 https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Overview-Management-High-Availability.htm?tocpath=Management%20High%20Availability%7C_____1#Overview_of_Management_High_Availability Pagina 468 - 471 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
19	Capacidades y cantidades	Throughput de Next Generation Firewall (NGFW) de 18 Gbps medido con tráfico productivo real.	los PA 3420 Soportan 19 Gbps https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series pag 5	CUMPLE		https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 3 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
20	Capacidades y cantidades	Throughput de Prevención de Amenazas o Threat Prevention Throughput de 10 Gbps medido con tráfico productivo real, con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), DNS Security, Filtro de Archivos, y Logging activo.	Los PA 3420 Soportan 10 Gbpshttps://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series pag 5	CUMPLE		https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 3 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
21	Capacidades y cantidades	Cada equipo debe tener la Capacidad de procesar mínimo 2.2 millones de conexiones de red simultáneas (concurrentes)	los PA 3420 Soportan 2,2 millones de sesiones https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series pag 5	CUMPLE		https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 3 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
22	Capacidades y cantidades	Cada equipo debe tener la Capacidad de procesar mínimo 200.000 nuevas conexiones en red por segundo.	los PA 3420 Soportan 220.000 nuevas conexiones por segundo https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series pag 5	CUMPLE		https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 3 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
23	Capacidades y cantidades	Cada equipo debe contar con dos fuentes en el rango de 110v-220v AC hot-swappable ofreciendo redundancia en el suministro eléctrico	Los equipos Pa3420 Soportan fuentes redundantes hotswap 450w AC https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series pag 6	CUMPLE		https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 4 del link	NO CUMPLE	Con el numero de parte o equipo ofertado no es posible validar el cumplimiento de la caracteristica tecnica.	https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
24	Capacidades y cantidades	Cada equipo debe incluir Disco de Estado Sólido (SSD) de mínimo 450 GB para almacenamiento del sistema y logs.	Los equipos PA3420 poseen disco SSD de 480Gb https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series Pag 6	CUMPLE		https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 3 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
25	Capacidades y cantidades	**Puertos de cobre:** Mínimo 8 Interfaces (1G/10G) RJ45 o (1G/10G) SFP+ de tráfico de red para cada equipo. (No debe incluir interfaces para alta disponibilidad, ni administración). **Nota:** En tal caso de que se dé cumplimiento incluyendo un módulo (1G/10G) SFP+, debe incluir como mínimo 4 optical transceiver SFP+ 10G Base-T RJ45 compatibles con el módulo.	Los pa 3420 poseen 12 1G/10G RJ45 https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series Pag 6	CUMPLE		https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 3 del link Se incluye en la oferta economica el modulo de expasion para las interfaces a 10Gbps en SFP+ adicional incluimos los 4 transceivers de 10Gb RJ45	NO CUMPLE	Con el numero de parte o equipo ofertado no es posible validar el cumplimiento de la caracteristica tecnica.	https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
26	Capacidades y cantidades	**Puertos de fibra**: Mínimo 8 Interfaces 10Gbps SFP/SFP+ de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración) incluyendo Mínimo 4 optical transceiver SFP+ 10-Gigabit multi-mode. **Nota:** Se debe tener en cuenta que dichas interfaces no deben ser las mismas requeridas para el punto 25.	Los pa 3420 poseen 10 1G/10G SFP/SFP+ https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series Pag 6	CUMPLE		https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 3 del link Se incluye en la oferta economica el modulo de expasion para las interfaces a 10Gbps con sus respectivos SFP+	NO CUMPLE	Con el numero de parte o equipo ofertado no es posible validar el cumplimiento de la caracteristica tecnica.	https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
27	Capacidades y cantidades	Mínimo 1 Interfaz adicional para alta disponibilidad mínimo a 1Gbps (No deben estar incluidas en las interfaces para tráfico de Red, ni administración)	Los pa 3420 poseen 2 interfaces de HA 100/1000 y 1 interfaz 10g SFP+ dedicada de HA HSCI https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series Pag 6	CUMPLE		https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 3 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
28	Capacidades y cantidades	Interfaz dedicada para administración 10/100/1000 para cada equipo	Los pa 3420 poseen 1 interfaz de administracion fuera de banda https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series Pag 6	CUMPLE		https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 3 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
29	Capacidades y cantidades	1 interfaz de tipo consola	Los pa 3420 poseen 1 interfaz RJ45 de consola y 1 micro USB de consola https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series Pag 6	CUMPLE		https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 3 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
30	Capacidades y cantidades	Capacidad de mínimo 60 zonas de seguridad.	Los pa 3420 poseen 200 zonas de seguridad https://www.paloaltonetworks.com/products/product-comparison?chosen=pa-3420	CUMPLE		Checkpoint no cuenta con un límite fijo en la cantidad de zonas, ya que son entidades lógicas diseñadas para agrupar segmentos de red que requieren para aplicar las politicas, por lo cual se podran creartantas zonas de seguridad como sean necesariaspara segmentar eficazmente la red de la entidad y de esta forma aplicar las políticas de seguridad de forma adecuada. https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_SecurityManagement_AdminGuide/CP_R81.20_Quantum_SecurityManagement_AdminGuide.pdf pagina 246 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
31	Servicios y protocolos de red	Etiquetas VLAN Tags 802.1Q por dispositivo / interfaz: 4094/4094	Los pa 3420 soportan vlan tag 4094/4094 por dospositivo e interfaz https://www.paloaltonetworks.com/products/product-comparison?chosen=pa-3420	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_Gaia_AdminGuide/CP_R81.20_Gaia_AdminGuide.pdf pagina 122 del link https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_Maestro_AdminGuide/CP_R81.20_Quantum_Maestro_AdminGuide.pdf pagina 129 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	CUMPLE	
32	Servicios y protocolos de red	Soporte de Agregación de links (LACP) 802.3ad	los equipos soportan lacp https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClG8CAK&lang=es%E2%80%A9	CUMPLE		https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 4 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
33	Servicios y protocolos de red	Debe soportar enrutamiento estático y dinámico (RIP, BGP y OSPFv2/v3) Para IPv4	Los equipos ofertados soportan enrutamientos dinamicos y estaticos IPV4 https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/static-routes/configure-a-static-route https://docs.paloaltonetworks.com/content/techdocs/en_US/pan-os/10-1/pan-os-networking-admin/rip.html https://docs.paloaltonetworks.com/content/techdocs/en_US/pan-os/10-1/pan-os-networking-admin/ospf.html https://docs.paloaltonetworks.com/content/techdocs/en_US/pan-os/10-1/pan-os-networking-admin/bgp.html	CUMPLE		https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 4 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
34	Servicios y protocolos de red	Debe soportar enrutamiento estático y dinámico (OSPFv3) Para IPv6	Los equipos ofertados soportan enrutamientos dinamicos y estaticos IPV6 https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/static-routes/configure-a-static-route https://docs.paloaltonetworks.com/content/techdocs/en_US/pan-os/10-1/pan-os-networking-admin/rip.html https://docs.paloaltonetworks.com/content/techdocs/en_US/pan-os/10-1/pan-os-networking-admin/ospf.htmlhttps://docs.paloaltonetworks.com/content/techdocs/en_US/pan-os/10-1/pan-os-networking-admin/bgp.html https://docs.paloaltonetworks.com/compatibility-matrix/reference/ipv6-support-by-feature	CUMPLE		https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf pagina 4 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
35	Servicios y protocolos de red	Capacidad de balancear varios enlaces de internet sin el uso de políticas específicas.	PANOS, Permite el balance de canales a traves de algoritmos de ECMP https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-networking-admin/ecmp/ecmp-load-balancing-algorithms	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SitetoSiteVPN_AdminGuide/Search.htm?q=balancing Pagina 172 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
36	Servicios y protocolos de red	Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QoS y SSL Decryption y protocolos de enrutamiento dinámico deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no hay contrato de licenciamiento con el fabricante.	Las funcionalidades mencionadas no requieren de suscripciones, estas son funcionalidades embebidas en los equipos y software PANOS https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/ipsec-vpn-basics https://docs.paloaltonetworks.com/network-security/security-policy/administration/all-policy-types/qos https://docs.paloaltonetworks.com/network-security/decryption/administration/decryption-overview	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SitetoSiteVPN_AdminGuide/Search.htm?q=SSL Pagina 15 del link https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Configuring-Mobile-Access-to-Network-Resources.htm?Highlight=%20SSL%20Decryption Pagina 225 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
37	Servicios y protocolos de red	Debe contar con modos NAT IPv4: IP estática, IP dinámica, IP y puerto dinámicos	Permite realizar Nat a traves de ip estatica, dinamica y puerto/Ip dinamico https://docs.paloaltonetworks.com/network-security/security-policy/administration/all-policy-types/nat	CUMPLE		https://www.checkpoint.com/es/cyber-hub/network-security/what-is-network-address-translation-nat/ https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Configuring-NAT-Policy.htm Pagina 299 del link https://support.checkpoint.com/results/sk/sk103656	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
38	Servicios y protocolos de red	Los NAT debe permitir reserva de IP dinámica, IP y puerto dinámicos con túnel y sobresuscripción.	Permite la reserva mencionada https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/nat/dynamic-ip-and-port-nat-oversubscription	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Overview-Management-High-Availability.htm? Pagina 613-614 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 37	https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
39	Control por política de firewall (aplicaciones, puertos y protocolos)	Soportar controles por zona de seguridad.	PANOS, permite generar controles por zonas de seguridad para segmentar la red y crear politicas con las mismas https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/getting-started/segment-your-network-using-interfaces-and-zones	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Security-Zones.htm?Highlight=zone%20controls Pagina 216 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
40	Control por política de firewall (aplicaciones, puertos y protocolos)	Controles de políticas por puerto y protocolo.	Permite la creacion de politicas con los compnentes de puerto y protocolo https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/security-policy/components-of-a-security-policy-rule#id5ac93939-77c9-4981-af21-965414779af3 https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/policy-objects	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Search.htm?q=Installing%20the%20Access%20Control%20Policy Pagina 288 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
41	Control por política de firewall (aplicaciones, puertos y protocolos)	Control de políticas por aplicaciones, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.	Pewrmite la creacion de politicas por aplicaciones Grupos de aplicaciones Dinamicos y categorias de aplicaciones https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/policy-objects	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Creating-Application-Control-and-URL-Filtering-Rules.htm?Highlight=Application%20Control Pagina 254 del link https://support.checkpoint.com/results/sk/sk52421	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
42	Control por política de firewall (aplicaciones, puertos y protocolos)	Identificación de la información de todas las aplicaciones que circulan por la red, en donde se evidencie puertos, protocolos, técnicas de evasión o cifrado.	Permite la identificacion y visualizacion de las aplicaciones con sus puertos y protocolos determinando sus categorias y capacidades https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/monitor-applications-and-threats https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-policy-rule-usage	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/HTTPS-Inspection.htm?Highlight=protoc#HTTPS_Inspection_on_Non-Standard_Ports Pagina 239, 461 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
43	Control por política de firewall (aplicaciones, puertos y protocolos)	Las políticas por aplicaciones deben contar con la capacidad de permitir, denegar, inspeccionar y tener control sobre el tráfico de las aplicaciones.	Permite definir en las politicas las capacidades de permitir , denegar y controlar el trafico sobre las aplicaciones definidas en las politicas https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/security-policy/security-policy-actions#id7e4a542a-1706-4f90-8bfa-ff15d24c53c1	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Search.htm?q=deny Pagina 288 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 116	https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
44	Control por política de firewall (aplicaciones, puertos y protocolos)	Etiquetado de aplicaciones por riesgo con el fin de identificar con mayor facilidad.	Se permite el bloqueo por pais https://live.paloaltonetworks.com/t5/community-blogs/geolocation-and-geoblocking/ba-p/315433	CUMPLE	La información se encuentra en el link proporcionado en el ítem 40	https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Search.htm?q=deny Pagina 288 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 93	https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
45	Control por política de firewall (aplicaciones, puertos y protocolos)	Soportar objetos y Reglas multicast.	Permite la creacion de reglas basada en objetos multicast: https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-networking-admin/ip-multicast/configure-ip-multicast	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Multicast-Access-Control.htm?Highlight=multicast pagina 297 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
46	Control por política de firewall (aplicaciones, puertos y protocolos)	Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.	Permite la configuracion de agendas asignadas a las politcas para que estas se habiliten o deshabiliten acorde a la agenda: https://docs.paloaltonetworks.com/network-security/security-policy/administration/objects/schedules	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Search.htm?q=deny Pagina 440-504 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 30	https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
47	Control por política de firewall (aplicaciones, puertos y protocolos)	Debe contener aprendizaje automático, con el fin de identificar y detener los intentos de ataques informáticos de día cero.	Los NGFw de Palo Alto Networks poseen aprendizaje de maquina con el find e detectar y detener el malware de dia zero In-Line https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/firewall-feature-overview-datasheet P2 y P18	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Search.htm?q=deny Pagina 253 - 259 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 30	https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
48	Control por política de firewall (aplicaciones, puertos y protocolos)	Debe contar con la funcionalidad de dar recomendaciones en las políticas creadas basado en buenas prácticas.	Posee Policy Optimizer quien permite listar las mejoras a las politicas de seguridad en linea https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/security-policy-rule-optimization https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices/security-policy-best-practices/deploy-security-policy-best-practices/policy-optimizer-best-practices Adicionalmente a traves de Strata Cloud manager Essentials (Free) se pueden realizar analisis de BPA a cada politica, revisar su integridad y ajustarlo a las practicas recomendadas por fabricante https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/overview/built-in-best-practices	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Search.htm?q=deny Pagina 320 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 30	https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
49	Control por política de firewall (aplicaciones, puertos y protocolos)	Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.	Las politicas de paloaltonetworks permiten el uso de los objetos mencionados para la creacion de las politicas https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/security-policy/components-of-a-security-policy-rule#id5ac93939-77c9-4981-af21-965414779af3	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Search.htm?q=deny Pagina 114, 245-348 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 30	https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
50	Control por política de firewall (aplicaciones, puertos y protocolos)	El sistema deberá tener la capacidad de reconocer aplicaciones, independiente del puerto y protocolo.	Al ser un NGFW de capa 7, una de sus grandes capacidades es la identificacion de aplicaciones independiente de puerto y protocolo que use https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/app-id/app-id-overview	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Creating-a-Basic-Access-Control-Policy.htm?Highlight=policy Pagina 281 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
51	Control por política de firewall (aplicaciones, puertos y protocolos)	Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.	para la creacion de politicas basadas en aplicaciones no es necesaria la definicion de los puertos y protocolos que use cada una https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/app-id/app-id-overview https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-rules	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Creating-a-Basic-Access-Control-Policy.htm?Highlight=policy Pagina 264 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
52	Control por política de firewall (aplicaciones, puertos y protocolos)	Detectar y limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD.	Los NGFW de palo alto permiten detectar y limitar el uso de ancho de banda por usuario, ip, aplicación https://docs.paloaltonetworks.com/network-security/quality-of-service/administration/prioritize-network-traffic-using-qos https://docs.paloaltonetworks.com/network-security/quality-of-service/administration/configure-qos	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Overview-Management-High-Availability.htm? Pagina 145 - 153 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 89	https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
53	Control por política de firewall (aplicaciones, puertos y protocolos)	Para mantener la seguridad de la red, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas.	los dispositivos NGFW de Palo alto permiten controlar las aplicaciones personalizadas y desconocidas https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/app-id/manage-custom-or-unknown-applications	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Search.htm?q=Firewall%20policy%20control Pagina 440 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
54	Control por política de firewall (aplicaciones, puertos y protocolos)	Permitir la restricción de usuarios sospechosos o malintencionados basado en comportamientos.	las politicas permiten crear grupos de usuarios dinamicos los cuales pueden identificar usuarios con comportamientos sospechosos y agregarlos a llistas negras https://docs.paloaltonetworks.com/network-security/security-policy/administration/objects/address-groups#use-dynamic-address-groups-in-policy-panorama	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/HTTPS-Inspection.htm?tocpath=HTTPS%20Inspection%7C_____0#HTTPS_Inspection Pagina 461 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
55	Prevención de amenazas	Para seguridad del ambiente contra ataques informáticos, el sistema de seguridad debe poseer módulo de IPS, Antivirus y Anti-Spyware integrados en los equipos que componen el sistema.	El licenciamiento posee advanced threat prevention quien es el modulo que posee las capacidades para prevencion de amenazas con IPS, AV, AntiSpyware https://www.paloaltonetworks.com/network-security/advanced-threat-prevention	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_ThreatPrevention_AdminGuide/CP_R81.20_ThreatPrevention_AdminGuide.pdf Pagina 259 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
56	Prevención de amenazas	El sistema debe soportar granularidad en las políticas de IPS Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos ítems.	las politicas permiten definir diferentes perfiles para analizar el trafico con perfiles de seguridad av, antuspyware, Vulnerability protection, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/security-profiles	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_ThreatPrevention_AdminGuide/CP_R81.20_ThreatPrevention_AdminGuide.pdf Pagina 259 - 263 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
57	Prevención de amenazas	Debe incluir seguridad contra ataques de denegación de servicios.	Los dispositivos de PaloAlto permiten crear perfiles de proteccion DOS https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/security-profiles	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_SecurityGateway_Guide/CP_R81.20_Quantum_SecurityGateway_AdminGuide.pdf Pagina 402 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
58	Prevención de amenazas	Debe permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, DNS, SMB, SMTP e POP3.	El perfil de seguridad Anvitivrus y AntiSpyware permite el bloqueo de ello en los protocolos mencionados https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-antivirus A nivekl de antispyware sobre todos trafico TCP y UDP https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-anti-spyware	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_ThreatPrevention_AdminGuide/CP_R81.20_ThreatPrevention_AdminGuide.pdf Pagina 90 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
59	Prevención de amenazas	Soportar bloqueo de archivos por tipo.	Permite la creacion de perfiles de bloqueo de archivos por tipo https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-file-blocking	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_ThreatPrevention_AdminGuide/CP_R81.20_ThreatPrevention_AdminGuide.pdf Pagina 374 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
60	Prevención de amenazas	Debe ser posible la configuración de diferentes políticas de control de amenazas y ataques basados en políticas del firewall donde cada política pueda incluir como mínimo: Usuarios, Grupos de usuarios, origen, destino, zonas de seguridad.	En las politicas todos los perfiles de control de amenazas se añaden a cada politica de seguridad que contiene cada objeto selector de trafico interesante https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/security-policy/components-of-a-security-policy-rule#id5ac93939-77c9-4981-af21-965414779af3	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_ThreatPrevention_AdminGuide/CP_R81.20_ThreatPrevention_AdminGuide.pdf Pagina 365 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
61	Prevención de amenazas	Debe ofrecer funcionalidades para análisis de Malware no conocidos incluidas en la propia herramienta.	Dentro del licenciamiento se ofrece Advanced Wildfire, quien permite la deteccion de malware no conocido https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-wildfire https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_ThreatPrevention_AdminGuide/CP_R81.20_ThreatPrevention_AdminGuide.pdf Pagina 81 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
62	Prevención de amenazas	Debe ser capaz de enviar archivos sospechosos transferidos de forma automática para análisis "In Cloud" o local, donde el archivo será ejecutado y simulado en un ambiente controlado.	Dentro del licenciamiento se ofrece Advanced Wildfire, quien permite el envio de analisis de archivos sospechosos https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-wildfire https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_ThreatPrevention_AdminGuide/CP_R81.20_ThreatPrevention_AdminGuide.pdf Pagina 80 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
63	Prevención de amenazas	Debe detener los ataques de inyección de día cero, exploits, botnets y Ataques Persistentes Avanzados (APT).	las capacidades de la suscrpcion Advanced Threat Prevention detienen ataques de dia cero, exploits, botnets, y APTs https://docs.paloaltonetworks.com/whats-new/new-features/may-2024/atp-support-for-zero-day-exploit-prevention	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_ThreatPrevention_AdminGuide/CP_R81.20_ThreatPrevention_AdminGuide.pdf Pagina 25 - 26 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
64	Prevención de amenazas	Las detenciones que realice el sistema deben estar basadas en comportamiento y IA.	El NGFW de Palo Alto Networks con Advanced Threat Prevention (ATP) incorpora Precision AI®, que combina machine learning, deep learning e inteligencia artificial generativa para analizar el tráfico en tiempo real y detener tanto amenazas conocidas como desconocidas de forma proactiva e inline, basándose en comportamiento y no solo en firmas. Además, integra funciones como Inline Cloud Analysis y Local Deep Learning para detección inmediata, Exfiltration Shield para bloquear exfiltración de datos vía DNS y capacidades avanzadas para identificar ataques generados por IA (LLMs), ofreciendo así una prevención integral y adaptativa frente a amenazas modernas. https://www.paloaltonetworks.com/network-security/advanced-threat-prevention	CUMPLE		https://www.checkpoint.com/es/cyber-hub/network-security/what-is-network-security/top-network-security-issues-threats-and-concerns/ Pagina: 292 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
65	Prevención de amenazas	Debe utilizar una red de Inteligencia Global que le permita beneficiarse de la información recogida por los esfuerzos de investigación del fabricante.	La Prevención de Amenazas de Palo Alto Networks se fortalece con la inteligencia global de Unit 42, que analiza continuamente datos de millones de dispositivos y comparte actualizaciones en tiempo real, permitiendo a los NGFW aprovechar la investigación del fabricante para detener amenazas conocidas y desconocidas.	CUMPLE	La información se encuentra en el link proporcionado en el item 55	https://www.checkpoint.com/es/cyber-hub/network-security/what-is-network-security/top-network-security-issues-threats-and-concerns/ Pagina: 464 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
66	Prevención de amenazas	Debe tener la capacidad de detectar software malicioso y tomar acciones para proteger el entorno.	La Prevención de Amenazas de Palo Alto Networks detecta y bloquea software malicioso mediante análisis en tiempo real, firmas dinámicas e inteligencia basada en IA, tomando acciones automáticas como bloqueo de archivos, conexiones o procesos para proteger el entorno https://www.paloaltonetworks.com/network-security/advanced-threat-prevention	CUMPLE		https://www.checkpoint.com/es/cyber-hub/network-security/what-is-network-security/top-network-security-issues-threats-and-concerns/ Pagina 308-309 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
67	Prevención de amenazas	Debe detectar y proteger de los ataques originarios desde la web, como por ejemplo la descarga de archivos comprometedores y ejecución de los mismo.	La Prevención de Amenazas de Palo Alto Networks protege contra ataques web al bloquear descargas maliciosas y la ejecución de archivos comprometidos, usando análisis avanzado, sandboxing en WildFire, análisis en línea, inteligencia global y mecanismos basados en IA. En otras palabras: si un archivo intenta entrar de "incógnito" con malas intenciones, el firewall lo intercepta antes de que ponga un pie en tu red e inteligencia global para detener amenazas antes de que impacten el entorno https://www.paloaltonetworks.com/network-security/wildfire https://www.paloaltonetworks.com/network-security/advanced-threat-prevention	CUMPLE		https://www.checkpoint.com/es/cyber-hub/network-security/what-is-network-security/top-network-security-issues-threats-and-concerns/ Pagina 284 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
68	Prevención de amenazas	Debe contar con un entorno de inspección de códigos, sitios web o archivos maliciosos.	La Prevención de Amenazas de Palo Alto Networks incorpora entornos de inspección avanzados como WildFire, que analiza en la nube o de forma local códigos, sitios web y archivos sospechosos mediante sandboxing y técnicas de IA https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/advanced-wildfire	CUMPLE		https://www.checkpoint.com/es/cyber-hub/network-security/what-is-network-security/top-network-security-issues-threats-and-concerns/ Pagina 428 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
69	Prevención de amenazas	El sistema debe estar en la capacidad de bloquear llamadas a servidores remotos en caso de ataques de día cero y amenazas persistentes. Con el fin de proteger los equipos que se pudiesen comprometer y realicen llamadas a servidores remotos desde la red de la Universidad.	con Advanced Url Filtering y advanced Threat prevention se puede bloquear el llamado a servidores de comando y control https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/how-url-filtering-works https://www.paloaltonetworks.com/network-security/advanced-threat-prevention	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_ThreatPrevention_AdminGuide/CP_R81.20_ThreatPrevention_AdminGuide.pdf Pagina 25 y 26 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
70	Prevención de amenazas	Debe contar con la protección a través de la resolución de direcciones DNS. Con el fin de identificar dominios maliciosos	La Prevención de Amenazas de Palo Alto Networks incluye el servicio de DNS Security, que utiliza inteligencia en la nube y machine learning para analizar consultas DNS en tiempo real, identificar y bloquear dominios maliciosos, generados por algoritmos (DGAs) o utilizados para comando y control (C2), protegiendo así a los usuarios antes de que se establezca la conexión. https://docs.paloaltonetworks.com/dns-security	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_ThreatPrevention_AdminGuide/CP_R81.20_ThreatPrevention_AdminGuide.pdf Pagina 164 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
71	Prevención de amenazas	Los eventos generados deben contener la posibilidad de conocer el país de origen y destino, IP de origen y destino, URL, usuario que lo ejecuto y demás información relevante para su identificación.	La Prevención de Amenazas de Palo Alto Networks, integrada con los NGFW , genera eventos detallados que incluyen país de origen/destino, IP, URL, aplicación, usuario y otros metadatos relevantes, permitiendo identificar rápidamente la naturaleza y el contexto de la amenaza para su análisis y respuesta. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/traffic-logs	CUMPLE		Los blades como Application Control, URL Filtering, Identity Awareness, Threat Prevention y IPS inspeccionan el tráfico y generan eventos detallados. Los logs se almacenan y visualizan en SmartConsole, SmartView Tracker o SmartEvent. El sistema utiliza bases de datos de geolocalización IP para mostrar país de origen/destino en los eventos. https://support.checkpoint.com/results/sk/sk126172 Mediante Identity Awareness y la integración con LDAP/AD, los eventos pueden mostrar el usuario/grupo que realizó la acción. https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_IdentityAwareness_AdminGuide/Content/Topics-IDAG/Identity-Conciliation-PDP.htm Pagina: 142 del link https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_SecurityGateway_Guide/Content/Topics-FWG/URL-Filtering-Blade.htm Pagina: 216 del link https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_SecurityManagement_AdminGuid	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
72	Filtrado URL	Debe ser posible crear políticas por usuario, grupo de usuario, IPs, redes y zonas de seguridad.	Las capacidades de las politicas de seguridad permiten crear politicas dedicadas para el fiultrado URL para el trafico interesante que puede estar basado en usuarios o grupos de usuarios, ips, zonas de seguridad o redes https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/url-filtering-overview https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/policy/security-policy/components-of-a-security-policy-rule	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/CP_R81_Quantum_SecurityManagement_AdminGuide.pdf Pagina 216-217 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
73	Filtrado URL	Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y control de quién está utilizando URLs a través de la integración con servicios de directorio, autentificación vía LDAP, Active Directory, E-Directory y base de datos local.	Las capacidades de las politicas de seguridad permiten crear politicas dedicadas para el fiultrado URL para el trafico interesante que puede estar basado en usuarios o grupos de usuarios, ips, zonas de seguridad o redes https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/url-filtering-overview https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/policy/security-policy/components-of-a-security-policy-rule	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Creating-Application-Control-and-URL-Filtering-Rules.htm?Highlight=URL%20filtering Pagina 167 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
74	Filtrado URL	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL.	El Advanced URL Filtering de Palo Alto Networks permite definir políticas de acceso basadas tanto en URLs específicas como en categorías de URL (por ejemplo, redes sociales, malware, adult, etc.), aplicando controles granulares para proteger a los usuarios y cumplir con políticas de seguridad o normativas. https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/url-categories	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Creating-Application-Control-and-URL-Filtering-Rules.htm?Highlight=URL%20filtering Pagina 288 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
75	Filtrado URL	Debe permitir al menos 60 categorías predefinidas de URLs, con la capacidad de crear categorías adicionales personalizadas, de acuerdo con las necesidades específicas de la entidad.	El Advanced URL Filtering de Palo Alto Networks incluye más de 60 categorías predefinidas de URL y permite crear categorías personalizadas, brindando a las organizaciones la flexibilidad de adaptar las políticas de navegación según sus necesidades específicas. https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/url-categories	CUMPLE		https://support.checkpoint.com/results/sk/sk174045 https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_HarmonyEndpointWebManagement_AdminGuide/CP_R81.20_Harmony_Endpoint_WebManagement_AdminGuide.pdf Pagina 114 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
76	Filtrado URL	Debe soportar la creación de categorías URL custom.	El Advanced URL Filtering de Palo Alto Networks soporta la creación de categorías URL personalizadas, permitiendo a la organización definir y gestionar listas específicas de sitios que complementen las categorías predefinidas. https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/url-categories	CUMPLE		https://sc1.checkpoint.com/documents/SMB_R81.10.X/AdminGuides_Locally_Managed/EN/Content/Search.htm?q=URL%20custom Pagina 459 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
77	Filtrado URL	Debe soportar la exclusión de URLs del bloqueo por categoría.	El Advanced URL Filtering de Palo Alto Networks permite la exclusión de URLs específicas dentro de una categoría bloqueada, otorgando flexibilidad para habilitar el acceso a sitios puntuales sin desactivar la protección general de esa categoría.Esto se puede realizar generando categorias custom de los listados a de URL a excluir https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/url-categories	CUMPLE		https://sc1.checkpoint.com/documents/SMB_R81.10.X/AdminGuides_Locally_Managed/EN/Content/Search.htm?q=URL%20custom Pagina 411 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
78	Filtrado URL	Las detenciones que realice la solución deben estar basadas en comportamiento y IA.	El Advanced URL Filtering de Palo Alto Networks utiliza machine learning en tiempo real e IA basada en comportamiento para detectar y bloquear automáticamente sitios maliciosos, incluso antes de que sean categorizados en la base de datos tradicional. https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/url-filtering-overview	CUMPLE		https://www.checkpoint.com/fr/downloads/resources/how-artificial-intelligence-helps-achieve-the-best-cyber-threat-prevention-rates-whitepaper.pdf Pagina 3-6 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
79	Filtrado URL	Debe contar con un sistema de inteligencia de amenazas para validar la reputación de las URLs e IPs solicitadas por los usuarios en la navegación.	El Advanced URL Filtering de Palo Alto Networks se integra con la inteligencia global de amenazas (PAN-DB y servicios en la nube) para validar en tiempo real la reputación de URLs e IPs solicitadas por los usuarios, bloqueando el acceso a sitios maliciosos o comprometidos.	CUMPLE	La información se encuentra en el link proporcionado en el item 55	Checkpoint utiliza ThreatCloud, una red global de inteligencia de amenazas que valida la reputación de URLs e IPs en tiempo real. El motor de URL Filtering y Anti-Bot consulta ThreatCloud para determinar si una URL o IP es maliciosa antes de permitir el acceso. https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ThreatPrevention_AdminGuide/Content/Topics-TPG/The_Check_Point_Threat_Prevention_Solution.htm?tocpath=The%20Check%20Point%20Threat%20Prevention%20Solution%7C_____0#The_Check_Point_Threat_Prevention_Solution Pagina 79 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
80	Filtrado URL	Debe permitir la creación de listas blancas y negras con el fin de agrupar URL, según de la necesidad de la Universidad	Las capacidades de la suscrpcion permiten la creacion de listas blancas mediante custom categories o excepciones https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/url-categories https://docs.paloaltonetworks.com/advanced-url-filtering/administration/configuring-url-filtering/url-category-exceptions#ide877dd1a-8fcd-44bb-9670-fd54c87b77ef	CUMPLE		Se pueden crear listas blancas y negras personalizadas en la configuración de URL Filtering. El administrador puede definir grupos de URLs permitidas o bloqueadas según la necesidad de la entidad. https://support.checkpoint.com/results/sk/sk92743 https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_SecurityManagement_AdminGuide/Content/Topics-SECMG/SmartConsole-Toolbars-Access-and-Threat-Tools.htm?Highlight=Whitelists%20 Pagina 44 - 35 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
81	Filtrado URL	Debe tener una base de datos de al menos 200 millones de URLs categorizadas o debe tener la capacidad de poder aplicar técnicas de aprendizaje de maquina (Machine Learning) localmente sobre los NGFW para poder identificar nuevas categorías, por ejemplo, sitios de phishing o malware, con la capacidad de poder bloquear los mismos.	El Advanced URL Filtering de Palo Alto Networks se basa en la base de datos PAN-DB, que contiene más de 200 millones de URLs categorizadas, y además utiliza machine learning local en los NGFW para identificar dinámicamente nuevas amenazas, como sitios de phishing o malware, bloqueándolos de inmediato incluso antes de su clasificación oficial.	CUMPLE	La información se encuentra en el link proporcionado en el item 78	Check Point ThreatCloud categoriza cientos de millones de URLs y utiliza motores de Machine Learning para identificar nuevas amenazas, incluyendo phishing y malware. El motor de clasificación dinámica basado en IA categoriza sitios web no reconocidos y bloquea automáticamente sitios peligrosos. https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RN/Content/Topics-RN/Whats-New.htm?Highlight=Machine%20Learning Pagina 11 y 12 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
82	Filtrado de datos	Permitir identificar y opcionalmente prevenir la transferencia de informaciones sensibles, incluyendo, mas no limitando al número de tarjetas de crédito, permitiendo la creación de nuevos tipos de datos vía expresión regular.	A traves de las capacidades dde bloqueo de archivos se pueden definir caracteristicas del mismo o contenido para evitar su transito con patrones de datos predefinidos co personalizados https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/policy/security-profiles/set-up-data-filtering/predefined-data-filtering-patterns	CUMPLE		El Software Blade de Data Loss Prevention (DLP) permite identificar y prevenir la transferencia de datos sensibles, incluyendo números de tarjetas de crédito y tipos de datos definidos por expresiones regulares. El administrador puede crear reglas DLP para detectar patrones específicos y bloquear o alertar sobre transferencias no autorizadas. https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_DataLossPrevention_AdminGuide/Content/Topics-DLPG/Introduction-to-Data-Loss-Prevention.htm?tocpath=Introduction%20to%20Data%20Loss%20Prevention%7C_____0 Pagina 12 - 25 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
83	Filtrado de datos	Permitir la detección de portales de phishing estableciendo políticas que eviten el envío de credenciales válidas de usuarios a sitios no autorizados.	las capacidades de filtrado URL permiten prevenir el ingreso de credenciales corporativas en categorias de sitios no autorizadas o maliciosas https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-features/credential-phishing-prevention	CUMPLE		El Software Blade Zero Phishing detecta portales de phishing y puede bloquear el envío de credenciales a sitios no autorizados. Analiza formularios web y bloquea el envío de credenciales a sitios sospechosos. https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_SecurityGateway_Guide/CP_R81.20_Quantum_SecurityGateway_AdminGuide.pdf Pagina 48 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
84	Filtrado de datos	Con el fin de proteger las credenciales de la comunidad Universitaria, debe evitar la filtración a sitios web de terceros y la reutilización de credenciales sustraídas mediante la habilitación de la autenticación de varios factores.	A traves de credential Phishing Prevention se puede evitar la filtracion de credenciales, adicionalmente se permite integrar con servicios a traves de SAML para adoptar capacidades de MFA https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-features/credential-phishing-prevention https://docs.paloaltonetworks.com/cloud-identity/cloud-identity-engine-getting-started/authenticate-users-with-the-cloud-identity-engine/configure-an-identity-provider-in-the-cloud-identity-engine	CUMPLE		Check Point soporta autenticación multifactor (MFA) para acceso remoto y VPN, pero la prevención de reutilización de credenciales sustraídas depende de la integración con soluciones externas de gestión de identidades. https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_RemoteAccessVPN_AdminGuide/Content/Topics-VPNRG/User-and-Client-Authentication.htm?Highlight=authentication Pagina 41 -46 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
85	Identificación de usuarios	Debe permitir integración con Radius, ldap, Active Directory, E-directory y base de datos local, para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.	La funcionalidad User-ID de Palo Alto Networks permite integrar el NGFW con Active Directory, LDAP, RADIUS, eDirectory y base de datos local, lo que habilita la identificación de usuarios y grupos para aplicar controles y políticas de seguridad con granularidad basada en identidad. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/authentication/authentication-types/ldap https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/authentication-types/radius	CUMPLE		Identity Awareness permite integración con todos estos servicios para identificación granular de usuarios y grupos. Permite crear políticas basadas en usuarios y grupos identificados por estos servicios. https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_IdentityAwareness_AdminGuide/CP_R81.20_IdentityAwareness_AdminGuide.pdf pagina: 36, 45, 184 y 192 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
86	Identificación de usuarios	Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x y soluciones NAC via syslog, para la identificación de direcciones IP y usuarios.	La funcionalidad User-ID de Palo Alto Networks soporta la recepción de eventos de autenticación vía syslog provenientes de controladoras inalámbricas, dispositivos 802.1X y soluciones NAC, permitiendo mapear direcciones IP con usuarios para aplicar políticas de seguridad basadas en identidad. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-id-to-monitor-syslog-senders-for-user-mapping	CUMPLE		Identity Awareness soporta la recepción de eventos de autenticación vía syslog para correlacionar IP y usuario. Permite correlacionar eventos de autenticación de dispositivos externos para identificar usuarios. https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_LoggingAndMonitoring_AdminGuide/Topics-LMG/Working-with-Syslog-Servers.htm Pagina 91 del ink	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
87	Identificación de usuarios	Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tienen estos servicios.	La funcionalidad User-ID de Palo Alto Networks incluye soporte para múltiples usuarios en una misma dirección IP en entornos como Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre aplicaciones y tráfico, incluso en sesiones compartidas. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-for-terminal-server-users/configure-the-palo-alto-networks-terminal-services-agent-for-user-mapping	CUMPLE		https://sc1.checkpoint.com/documents/Identity_Awareness_Clients_Admin_Guide/Content/Topics-IA-Clients-AG/Identity-Agent-for-Terminal-Server-Configuring.htm?Highlight=citrix https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_IdentityAwareness_AdminGuide/Content/Topics-IDAG/Identity-Sources-Terminal-Servers.htm?Highlight=Terminal%20Server Pagina 35 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
88	Identificación de usuarios	Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows.	La funcionalidad User-ID de Palo Alto Networks soporta la identificación de múltiples usuarios en una misma IP incluso en servidores accedidos remotamente que no sean Windows, mediante agentes como Terminal Services Agent y mapeo de usuarios vía syslog o integración con directorios, garantizando control granular en entornos heterogéneos. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/user-id	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/Topics-IDAG/Identity-Sources-Terminal-Servers.htm?Highlight=%20Windows%20servers Pagina 104 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
89	Calidad de servicio	Como la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube, ustream, etc.) y tener un alto consumo de ancho de banda, el sistema debe controlarlas por políticas de máximo ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones.	La funcionalidad de Quality of Service (QoS) en los NGFW de Palo Alto Networks permite controlar aplicaciones y tráfico de alto consumo aplicando políticas de QoS máximo por usuario, grupo o aplicación, garantizando una distribución eficiente de los recursos de red. https://docs.paloaltonetworks.com/network-security/quality-of-service/administration/prioritize-network-traffic-using-qos	CUMPLE		Se utiliza el blade de Application Control junto con QoS para identificar aplicaciones (como YouTube) y aplicar políticas de ancho de banda. Se puedelimitar el ancho de banda máximo por aplicación, usuario, grupo, dirección IP, etc. Ejemplo: Crear una regla QoS que limite el ancho de banda para YouTube a 1 Mbps por usuario. https://support.checkpoint.com/results/sk/sk30590 https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_QoS_AdminGuide/Content/Topics-QoSG/Introduction-to-QoS.htm?Highlight=application https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_QoS_AdminGuide/Content/Topics-QoSG/Advanced-QoS-Policy-Management.htm?Highlight=Bandwidth%20Limits#Examples__Guarantees_and_Limits https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/CP_R81_Quantum_SecurityManagement_AdminGuide.pdf Pagina 254 - 257 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
90	Calidad de servicio	Las VPN deberán estar en la capacidad o tener disponible en futuras actualizaciones la capacidad de configurar PPK poscuánticas en IKEv2, basadas en el estándar RFC 8784 o en el presente a través de la actualización de certificados a una longitud de 4096 bits RSA, tal como lo sugiere el NIST.	Las VPN de Palo Alto Networks en PAN-OS 11.1 y versiones posteriores ya soportan la configuración de claves precompartidas postcuánticas (PPK) según el estándar RFC 8784, lo que permite proteger IKEv2 contra futuros ataques cuánticos mediante el uso de una clave entregada fuera del canal y mezclada durante el intercambio de claves. Además, el sistema permite actualizar a certificados RSA de 4096 bits, siguiendo las recomendaciones de seguridad del NIST. https://docs.paloaltonetworks.com/network-security/quantum-security/administration/configure-quantum-resistant-ikev2-vpns/configure-post-quantum-ikev2-vpns https://docs.paloaltonetworks.com/whats-new/new-features/november-2023/post-quantum-ike-vpn-support	CUMPLE		Check Point soporta certificados RSA de hasta 4096 bits para VPN, cumpliendo la recomendación NIST. Desde la versión R75, Check Point permite el uso de certificados RSA de 4096 bits para VPN y portales. Esto cumple con la recomendación de NIST para robustez criptográfica. https://support.checkpoint.com/results/sk/sk96591 R82 agrega soporte para el algoritmo ML-KEM (Kyber768), conforme al estándar FIPS 203, para proteger el tráfico VPN contra ataques futuros de computación cuántica. Este soporte está orientado a la protección poscuántica, aunque no menciona explícitamente RFC 8784 (PPK en IKEv2), pero sí la adopción de algoritmos recomendados por NIST para criptografía poscuántica. https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RN/Content/Topics-RN/Whats-New.htm?Highlight=IPSec Pagina 15 y 16 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
91	Calidad de servicio	Soportar la creación de políticas de QoS por: * Dirección de origen * Dirección de destino * Por usuario y grupo de LDAP/AD * Por aplicaciones * Por puerto	El QoS de Palo Alto Networks permite la creación de políticas flexibles de control de tráfico basadas en múltiples criterios, lo que garantiza granularidad en la asignación y limitación de ancho de banda. https://docs.paloaltonetworks.com/pan-os/11-2/pan-os-web-interface-help/policies/policies-qos	CUMPLE		El blade de QoS permite crear reglas basadas en: Dirección de origen/destino (IP, red) Usuario/grupo (integración con LDAP/AD) Aplicaciones (usando Application Control) Puerto (servicio TCP/UDP) https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_QoS_AdminGuide/Content/Topics-QoSG/Basic-Policy-Management.htm?Highlight=group Pagina 50 - 57 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
92	Calidad de servicio	El QoS debe permitir la definición de clases por: * Ancho de banda garantizado * Ancho de banda máxima * Cola de prioridad.	El QoS en los NGFW de Palo Alto Networks permite definir clases de tráfico configurando parámetros como ancho de banda garantizado, ancho de banda máximo y colas de prioridad, lo que asegura un uso eficiente de los recursos y priorización de aplicaciones críticas. https://docs.paloaltonetworks.com/network-security/quality-of-service/administration/configure-qos https://docs.paloaltonetworks.com/network-security/quality-of-service/administration/qos-concepts-for-traffic-control	CUMPLE		QoS de Check Point permite definir: * Ancho de banda garantizado: Reserva mínima para una clase/regla. * Ancho de banda máximo: Límite superior para una clase/regla. * Cola de prioridad: Asignación de prioridad (Weighted Fair Queuing, Low Latency Queuing). https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_QoS_AdminGuide/Topics-QoSG/Advanced-QoS-Policy-Management.htm?Highlight=queue Pagina 58-64 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
93	Calidad de servicio	Soportar priorización RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.	El QoS de Palo Alto Networks soporta la priorización en tiempo real de protocolos de voz (VoIP) como H.323, SIP, SCCP, MGCP, así como aplicaciones de colaboración como Skype, asegurando baja latencia y calidad en las comunicaciones críticas.	CUMPLE	La información se encuentra en el link proporcionado en el ítem 52	https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_SecurityManagement_AdminGuide/CP_R81.20_Quantum_SecurityManagement_AdminGuide.pdf pagina 249 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
94	Calidad de servicio	Soportar marcación de paquetes de servicios diferenciados (Diffserv)	El QoS en Palo Alto Networks soporta la marcación de paquetes con DiffServ (DSCP/ToS bits), lo que permite integrar las políticas de priorización del firewall con mecanismos de calidad de servicio en toda la red para garantizar un tratamiento consistente del tráfico. https://docs.paloaltonetworks.com/network-security/quality-of-service/administration/enforce-qos-based-on-dscp-classification	CUMPLE		https://support.checkpoint.com/results/sk/sk32176 https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_QoS_AdminGuide/CP_R82_QoS_AdminGuide.pdf Pagina 62 - 69 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
95	VPN embebida	Debe soportar VPN IPSec Nativa Client-To-Site y Site-to-Site (Incluyendo conexión Site-to-Site con infraestructuras en la nube mínimo con: Amazon, Microsoft Azure)	Los NGFW de Palo Alto Networks soportan VPN IPsec nativa tanto Client-to-Site como Site-to-Site, incluyendo compatibilidad con infraestructuras en la nube como Amazon AWS y Microsoft Azure, lo que asegura conectividad segura entre usuarios remotos, sedes y entornos cloud híbridos. https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/ipsec-vpn-basics/ipsec-vpn https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-quick-configs/remote-access-vpn-certificate-profile	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/SmartConsole-Toolbars-Access-and-Threat-Tools.htm?Highlight=Data%20filtering pagina 430 del link https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_SitetoSiteVPN_AdminGuide/Content/Topics-VPNSG/VPN-Tunnel-with-Cloud.htm Pagina 209 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
96	VPN embebida	La VPN IPSEc debe soportar mínimo: * Cifrado 3DES * Cifrado AES (128 bits, 256 bits) * Autenticación: MD5, SHA-1, SHA-256, SHA-384, SHA-512 * Intercambio de calves: clave manual, IKEv1 e IKEv2 * Autenticación vía certificado IKE PKI.	La VPN IPsec de Palo Alto Networks soporta estándares avanzados de seguridad, incluyendo cifrado 3DES y AES (128/256 bits), algoritmos de autenticación MD5, SHA-1, SHA-256, SHA-384 y SHA-512, métodos de intercambio de claves mediante clave manual, IKEv1 e IKEv2, además de autenticación basada en certificados IKE y PKI, garantizando interoperabilidad y cumplimiento con buenas prácticas de seguridad. https://docs.paloaltonetworks.com/compatibility-matrix/reference/supported-cipher-suites/cipher-suites-supported-in-pan-os-11-2/cipher-suites-supported-in-pan-os-11-2-ipsec	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SitetoSiteVPN_AdminGuide/Topics-VPNSG/IPsec-and-IKE.htm?Highlight=aes IPsec and IKE Pagina 47 del link	CUMPLE		https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-3100-series-ds.pdf	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
97	VPN embebida	Debe poseer interoperabilidad VPN IPSec mínimo con los siguientes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet, Sonic Wall.	Los NGFW de Palo Alto Networks ofrecen interoperabilidad VPN IPsec con múltiples fabricantes de seguridad de red, garantizando la conectividad segura en entornos híbridos y con infraestructura heterogénea. https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/get-started-with-ipsec-vpn-site-to-site/site-to-site-vpn-overview	CUMPLE		https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_SitetoSiteVPN_AdminGuide/html_frameset.html https://community.checkpoint.com/t5/Security-Gateways/IPSec-VPN-tunnel-with-Fortinet/m-p/241755#M46941 https://support.checkpoint.com/results/sk/sk108600	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
98	VPN embebida	Permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operativo del equipo cliente o por medio de interfaz WEB.	La VPN embebida en los NGFW de Palo Alto Networks, mediante GlobalProtect, permite a los usuarios conectarse de forma segura ya sea a través de un cliente instalado en el sistema operativo (Windows, macOS, Linux, iOS, Android) o mediante una interfaz web SSL, ofreciendo flexibilidad de acceso remoto. https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-overview	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/Topics-FWG/Kernel-Debug/Module-VPN.htm Pagina: 356 - 358 del link https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/Topics-FWG/Remote-Access-VPN.htm Pagina: 26 del link https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_RemoteAccessVPN_AdminGuide/Topics-VPNRG/Check-Point-VPN.htm Pagina: 18-19 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
99	VPN embebida	Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.	La autenticacion de usuarios a traves de global protect permite realizarce de multiples perfiles de autenticacion https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-user-authentication	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/LDAP-Servers-Configuring-Admins-Users.htm Pagina: 149-153 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 116	No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
100	VPN embebida	Permite establecer un túnel VPN client-to-site del cliente al sistema de seguridad, proveyendo una solución de single-sign-on a los usuarios, integrándose como las herramientas de Windows-logon	La VPN Client-to-Site con GlobalProtect de Palo Alto Networks permite establecer túneles seguros entre el cliente y el firewall, ofreciendo integración con Windows Logon para Single Sign-On (SSO), lo que facilita a los usuarios autenticarse de forma transparente al iniciar sesión en su equipo. https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-user-authentication	CUMPLE		https://learn.microsoft.com/en-us/entra/identity/saas-apps/check-point-remote-access-vpn-tutorial	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
101	VPN embebida	Debe permitir que las conexiones VPN SSL o VPN IPSec sean establecidas de las siguientes formas: * Antes o durante la autenticación del usuario en la estación * Después de la autenticación del usuario en la estación * Manualmente por el usuario	La VPN de Palo Alto Networks con GlobalProtect permite establecer conexiones SSL o IPsec de distintas formas: antes o durante la autenticación en el equipo (pre-logon), después de que el usuario se autentique (on-demand), o manualmente iniciado por el usuario, brindando flexibilidad en el acceso remoto seguro. https://docs.paloaltonetworks.com/globalprotect/5-2/globalprotect-app-user-guide/globalprotect-app-for-windows/use-connect-before-logon-followed-by-the-authentication-method	CUMPLE		https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RemoteAccessVPN_AdminGuide/Content/Topics-VPNRG/Check-Point-VPN.htm Pagina: 15 - 28 del link https://support.checkpoint.com/results/sk/skl5130 Configuración en SmartDashboard: Regla con acción "Client Auth" en modo parcialmente automático o manual https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_CLI_ReferenceGuide/Content/Topics-CLIG/VPNSG/vpn-tu-del.htm https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_RemoteAccessVPN_AdminGuide/CP_R81.10_RemoteAccessVPN_AdminGuide.pdf Pagina 17 - 31 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
102	VPN embebida	El cliente de VPN client-to-site debe ser compatible al menos con: Windows 8, Windows 10, Windows 11 y últimas versiones de Mac.	Las versiones anteriores a Win8 permiten se usadas a traves de agentes de global protect version 5.x que poseen EOL, Mientras las versiones windows 10 o superior son compatibles con las versiones 6,x en adelante https://docs.paloaltonetworks.com/compatibility-matrix/reference/globalprotect/where-can-i-install-the-globalprotect-app	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_RemoteAccessVPN_AdminGuide/Content/Topics-VPNRG/Remote-Access-Solutions.htm?Highlight=macOS Pagina 28 - 36 del link https://support.checkpoint.com/results/sk/sk67820	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
103	VPN embebida	Capacidad de soportar mínimo 1800 clientes de VPN SSL (Client) simultáneos sin generar costos adicionales a la solución de seguridad perimetral. La VPN SSL deberá permitir mínimo la creación del túnel seguro y la conexión entre la red corporativa y el endpoint del usuario sin implementar características de cumplimiento o postura.	El dispositivo Ofertado posee la capacidad de generar maximo 1800 tuneles de VPN https://www.paloaltonetworks.com/products/product-comparison?chosen=pa-3420	CUMPLE		https://support.checkpoint.com/results/sk/sk67820 https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf Pagina 2 y 3 del link Ver sección "VPN Throughput" y "Concurrent Connections"	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
104	VPN embebida	Capacidad de soportar mínimo 1000 túneles de VPN IPSEC (Site to Site) simultáneos sin generar costos adicionales a la solución de seguridad perimetral. La VPN IPSEC deberá permitir mínimo la creación del tunel seguro y la conexión entre las redes corporativas sin implementar características de cumplimiento o postura.	El dispositivo ofertado posee la capacidada de generar hasta 5000 Vpns S2s https://www.paloaltonetworks.com/products/product-comparison?chosen=pa-3420	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_SitetoSiteVPN_AdminGuide/Content/Topics-VPNSG/Basic-Site-to-Site-VPN-Configuration.htm Pagina: 248 - 249 del link	NO CUMPLE	En el link no se visualiza el valor minimo de clientes VPN tuneles IPSEC	No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
105	VPN embebida	Throughput de VPN de mínimo 9 Gbps IPsec.	El dispositivo ofertado posee la capacidad de Throughput de VPN de hasta 9,9Gbps https://www.paloaltonetworks.com/products/product-comparison?chosen=pa-3420	CUMPLE		Ver Datasheeet "VPN AES-GCM 1452B [Gbps] 75" https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf Pagina: 3 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
106	DNS Security	La solución compuesta por dos equipos para garantizar la alta disponibilidad (HA), debe ser alimentada por un servicio de inteligencia global capaz de identificar millones de dominios maliciosos con análisis en tiempo real sin depender de firmas estáticas.	La suscripción de DNS Security en los NGFW de Palo Alto Networks aprovecha la inteligencia global de Unit 42 y análisis en tiempo real con machine learning en la nube, lo que permite identificar y bloquear millones de dominios maliciosos sin depender de firmas estáticas. https://docs.paloaltonetworks.com/dns-security	CUMPLE		Check Point Quantum 9700 está alimentado por ThreatCloud AI, una red global con más de 150,000 sensores que analiza millones de indicadores de compromiso (IoCs) en tiempo real. Utiliza machine learning y deep learning para detectar amenazas sin depender de firmas estáticas. https://www.checkpoint.com/ai/threatcloud/ https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_ThreatPrevention_AdminGuide/CP_R81.20_ThreatPrevention_AdminGuide.pdf pagina 91 , 272, 326 del link https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf Pagina: 1 AI/ML powered Threat Prevention	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
107	DNS Security	El servicio de protección de DNS debe poder habilitarse sin modificar la configuración de DNS de la red local o desviar el tráfico DNS a servidores externos.	La suscripción de DNS Security en los NGFW de Palo Alto Networks se habilita directamente en el firewall, sin necesidad de cambiar la configuración de los servidores DNS locales ni desviar el tráfico a servidores externos, lo que simplifica la implementación y asegura la protección sin impacto en la red existente. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/advanced-dns-security https://docs.paloaltonetworks.com/dns-security/administration/configure-dns-security/enable-advanced-dns-security	CUMPLE		La protección DNS se habilita en el gateway, inspeccionando el tráfico DNS sin necesidad de cambiar la configuración de los servidores DNS internos ni redirigir el tráfico a servidores externos. https://support.checkpoint.com/results/sk/sk34295	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
108	DNS Security	La solución compuesta por dos equipos para garantizar la alta disponibilidad (HA), debe ser un servicio que funcione integrado en la plataforma de NGFW, sin requerir adicionar hardware adicional y sin impactar el rendimiento del NGFW.	La suscripción de DNS Security de Palo Alto Networks se integra de forma nativa en la plataforma NGFW, sin necesidad de hardware adicional ni impacto en el rendimiento, ya que aprovecha la inspección de DNS existente del firewall. https://www.paloaltonetworks.com/network-security/advanced-dns-security	CUMPLE		La protección DNS y Threat Prevention funcionan como blades integrados en la plataforma NGFW, sin requerir hardware adicional y con optimización de rendimiento. https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf Pagina: 7 del link https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RN/Content/Topics-RN/Supported-Environments.htm#Standalone_and_Full_High_Availability Pagina 38 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
109	DNS Security	El servicio de protección de DNS debe alimentarse de múltiples fuentes de inteligencia de amenazas actualizadas en tiempo real, incluyendo telemetría de comportamiento de usuarios o dispositivos, y/o información proveniente de fuentes externas confiables y reconocidas internacionalmente	La suscripción de DNS Security de Palo Alto Networks se alimenta de múltiples fuentes de inteligencia en tiempo real, combinando telemetría global de dispositivos y usuarios con el análisis avanzado de Unit 42 e información de fuentes externas reconocidas internacionalmente, lo que garantiza una detección más precisa de dominios maliciosos. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/advanced-dns-security	CUMPLE		ThreatCloud se alimenta de múltiples fuentes, incluyendo telemetría de comportamiento y fuentes externas reconocidas internacionalmente. https://support.checkpoint.com/results/sk/sk175623 https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_ThreatPrevention_AdminGuide/Topics-TPG/Configuring-a-Malware-DNSTrap.htm?TocPath=Creating%20Threat%20Prevention%20Rules%7C_____7 Pagina: 92 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
110	DNS Security	La solución compuesta por dos equipos para garantizar la alta disponibilidad (HA), debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (DGA).	La suscripción de DNS Security de Palo Alto Networks utiliza machine learning en la nube para predecir y bloquear dominios maliciosos generados dinámicamente (DGA) https://docs.paloaltonetworks.com/content/dam/techdocs/es_ES/pdf/dns-security/dns-security-administration-es-es.pdf	CUMPLE		El Anti-Bot blade detecta y bloquea dominios generados por algoritmos DGA usando inteligencia global y machine learning. https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_RN/CP_R81.20_ReleaseNotes.pdf Pagina 12 del link https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ThreatPrevention_AdminGuide/CP_R82_ThreatPrevention_AdminGuide.pdf Pagina 77 del link Malware DNS Trap identifica clientes comprometidos que intentan acceder a dominios maliciosos conocidos. Al activar esta función, el puerto de enlace no bloquea las solicitudes DNS identificadas como maliciosas. La respuesta se manipula y se devuelve una dirección IP falsa al cliente. Con Malware DNS Trap, puede detectar clientes comprometidos revisando los registros con los intentos de conexión a la dirección IP falsa. Se bloquean las conexiones consecutivas dirigidas a la IP falsa. https://sc1.checkpoint.com/documents/R81.20/SmartEndpoint_OLH/EN/CP_R81.20_Harmony_Endpoint_Server_AdminGuide.pdf	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
111	DNS Security	Debe utilizar machine learning y/o inteligencia artificial para detectar nuevos dominios nunca vistos autogenerados por algoritmos DGA	La suscripción de DNS Security en los NGFW de Palo Alto Networks emplea machine learning e inteligencia artificial para identificar y bloquear en tiempo real dominios nunca antes vistos generados por algoritmos DGA, anticipándose a amenazas emergentes sin depender de firmas. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/advanced-dns-securityhttps://docs.paloaltonetworks.com/dns-security/administration/about-dns-security/cloud-delivered-dns-signatures	CUMPLE		DGA ML protection utiliza machine learning para identificar aproximadamente 500 nuevos dominios sospechosos por día. Con ThreatCloud se incluye protección basada en aprendizaje automático para identificar DGA. La base de datos del modelo de aprendizaje automático se basa en técnicas y URL conocidas de DGA (incluidos los hallazgos de DGALab). Mediante el uso de datos e información de WHOIS, feeds DNS y productos de Check Point en todo el mundo, el modelo proporciona un veredicto preciso sobre el dominio sospechoso. https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_RN/CP_R81.20_ReleaseNotes.pdf Pagina 12 del link https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ThreatPrevention_AdminGuide/CP_R82_ThreatPrevention_AdminGuide.pdf Pagina 77 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
112	DNS Security	Debe poseer políticas para bloquear dominios DGA o interrumpir las consultar de DNS a dichos dominios.	La suscripción de DNS Security de Palo Alto Networks permite aplicar políticas de seguridad que bloquean dominios generados por DGA o interrumpen las consultas DNS hacia dichos dominios, asegurando la prevención temprana de comunicaciones de malware. https://docs.paloaltonetworks.com/dns-security/administration/about-dns-security	CUMPLE		Se pueden definir políticas para bloquear o interrumpir consultas DNS a dominios DGA mediante el Anti-Bot blade(Prevenir el acceso a sitios maliciosos conocidos y verificar el comportamiento del tráfico). https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_RN/CP_R81.20_ReleaseNotes.pdf Pagina 12 del link https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ThreatPrevention_AdminGuide/CP_R82_ThreatPrevention_AdminGuide.pdf Pagina 77 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
113	DNS Security	Debe detectar e interrumpir robo de datos ocultos o tunelizados en tráfico DNS.	La suscripción de DNS Security de Palo Alto Networks detecta y bloquea intentos de exfiltración de datos ocultos o tunelizados en el tráfico DNS, interrumpiendo de forma proactiva estas técnicas de evasión sin afectar la resolución legítima de dominios. https://docs.paloaltonetworks.com/content/dam/techdocs/es_ES/pdf/dns-security/dns-security-administration-es-es.pdf	CUMPLE		El IPS blade y Threat Prevention detectan y bloquean intentos de tunelización y exfiltración de datos por DNS. https://blog.checkpoint.com/security/preventing-dns-tunneling-with-artificial-intelligence/ Pagina: No aplica	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
114	DNS Security	Debe analizar las consultas de DNS, incluyendo las tasas de consultas y patrones, entropía y frecuencia de n-grams o DGA Bajo Machine Learning / Artificial Intelligence para detectar posibles intentos de tunelización.	La suscripción de DNS Security de Palo Alto Networks analiza las consultas DNS utilizando machine learning e inteligencia artificial, evaluando tasas de consultas, patrones, entropía y frecuencia de n-grams para identificar posibles intentos de tunelización o exfiltración de datos, incluso cuando se usan dominios dinámicos generados por DGA. https://docs.paloaltonetworks.com/content/dam/techdocs/es_ES/pdf/dns-security/dns-security-administration-es-es.pdf Pag10	CUMPLE		El motor de ThreatCloud y Anti-Bot blade analizan patrones, tasas y entropía de consultas DNS usando ML/IA para detectar tunelización y DGA. https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_RN/CP_R81.20_ReleaseNotes.pdf Pagina 12 del link https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ThreatPrevention_AdminGuide/CP_R82_ThreatPrevention_AdminGuide.pdf Pagina 77 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
115	DNS Security	Debe permitir como acción ante peticiones DNS maliciosas: alertar, bloquear las conexiones y además responder a la petición con IP sumidero (sinkhole) con el fin de identificar al usuario/equipo realizando consultas DNS maliciosas.	La suscripción de DNS Security de Palo Alto Networks permite que, ante consultas DNS maliciosas, el sistema genere alertas, bloquee las conexiones y responda con un sinkhole, lo que facilita identificar al usuario o equipo que realiza las consultas maliciosas y prevenir propagación de malware. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/advanced-dns-security Pag4	CUMPLE		mediante el blade de Threat Prevention y la funcionalidad DNS Trap, permite: Alertar sobre consultas DNS maliciosas. Bloquear la conexión. Responder con una IP sumidero (sinkhole) para identificar el equipo o usuario que realiza la consulta. https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_ThreatPrevention_AdminGuide/Content/Topics-TPG/Configuring-a-Malware-DNSTrap.htm?Highlight=Configuring%20a%20Malware%20DNS%20Trap Pagina: 131 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
116	DNS Security	Debe clasificar los dominios maliciosos en categorías específicas asociadas al tipo de riesgo, como, por ejemplo: malware, DGA, DNS tunneling, Comando y Control, DNS dinámicos, phising o dominios recientemente registrados.	La suscripción de DNS Security de Palo Alto Networks clasifica los dominios maliciosos en categorías específicas según el tipo de riesgo, incluyendo malware, DGA, DNS tunneling, comando y control (C2), DNS dinámicos, phishing y dominios recién registrados, facilitando un análisis más preciso y acciones de mitigación adecuadas. https://docs.paloaltonetworks.com/content/dam/techdocs/es_ES/pdf/dns-security/dns-security-administration-es-es.pdf Pag9 en adelante	CUMPLE		Se utiliza ThreatCloud AI, que clasifica los dominios maliciosos en categorías. Esta clasificación permite aplicar políticas diferenciadas por tipo de amenaza. https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_RN/CP_R81.20_ReleaseNotes.pdf Pagina: 12 del link https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_ThreatPrevention_AdminGuide/CP_R82_ThreatPrevention_AdminGuide.pdf Pagina: 77 del link https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_SecurityManagement_AdminGuide/CP_R81.20_Quantum_SecurityManagement_AdminGuide.pdf Pagina 479 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
117	DNS Security	Debe perimir la acción a tomar dependiendo de la categoría a la que pertenezca el dominio, pudiendo tomar acciones diferentes para cada tipo de categoría.	La suscripción de DNS Security de Palo Alto Networks permite definir acciones específicas según la categoría del dominio, de modo que se puedan aplicar diferentes medidas de seguridad (alertar, bloquear, sinkhole) según si se trata de malware, DGA, phishing u otras categorías de riesgo.	CUMPLE	La información se encuentra en el link proporcionado en el ítem 107	Se permite definir políticas de seguridad que pueden tomar diferentes acciones dependiendo de la categoría a la que pertenezca el dominio. Por ejemplo, puede bloquear el acceso a dominios clasificados como phishing, mientras que puede permitir el acceso a dominios que son seguros. Esto se logra a través de la configuración de reglas en el firewall que se basan en la categorización de los dominios. https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_SecurityManagement_AdminGuide/CP_R81.20_Quantum_SecurityManagement_AdminGuide.pdf Pagina: 294 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
118	DNS Security	La solución compuesta por dos equipos para garantizar la alta disponibilidad (HA), debe brindar el contexto de cada dominio incluyendo historial completo para informar el origen y reputación de cada dominio.	La suscripción de DNS Security de Palo Alto Networks, en configuraciones de alta disponibilidad (HA), proporciona contexto completo de cada dominio, incluyendo historial, origen y reputación, lo que permite un análisis detallado y decisiones de seguridad informadas. https://docs.paloaltonetworks.com/content/dam/techdocs/es_ES/pdf/dns-security/dns-security-administration-es-es.pdf Pag11	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Domains.htm?Highlight=DNS%20Security Pagina: 212 link https://www.checkpoint.com/downloads/products/quantum-force-9700-datasheet.pdf Pagina: 2 link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
119	Consola de administración y monitoreo	El sistema debe incluir consola de administración y monitoreo, incluyendo el licenciamiento de software necesario para las dos funcionalidades, como también el hardware dedicado para el funcionamiento de las mismas	La consola de administración y monitoreo de Palo Alto Networks, mediante Panorama, permite centralizar la gestión de políticas y la supervisión de múltiples NGFW, incluyendo el licenciamiento de software necesario y el hardware dedicado para asegurar el funcionamiento óptimo de la administración y el monitoreo. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/monitoring https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/firewall-administration	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Search.htm?q=Administration%20and%20monitoring%20console%20 Pagina 53 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 93	No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
120	Consola de administración y monitoreo	La consola de administración y monitoreo puede residir en el mismo appliance de seguridad de red, desde que posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función.	La consola de administración y monitoreo puede residir directamente en el appliance NGFW, siempre que se cuente con recursos dedicados de CPU, memoria, interfaces de red y sistema operativo para esta función, asegurando gestión y monitoreo eficientes sin afectar el rendimiento del firewall. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/monitoring	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Creating-Application-Control-and-URL-Filtering-Rules.htm?Highlight=Application%20Control Pagina 254 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 93	No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
121	Consola de administración y monitoreo	La administración del sistema debe soportar acceso vía SSH, cliente WEB (HTTPS) y API abierta	Los Ngfw de palo alto poseen la capacidad de gestionarse a traves de SSH o HTTPS incluyendo gestion a traves de APIS https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/firewall-administration/management-interfaces	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Assigning-Permission-Profiles-to-Administrators.htm?Highlight=Administration%20and%20monitoring%20console%20 Pagina: 77-79 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 128	No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
122	Consola de administración y monitoreo	La administración en la consola debe permitir/hacer: * Creación y administración de políticas de firewall y control de aplicaciones * Creación y administración de políticas de IPS y Anti-Spyware * Creación y administración de políticas de filtro de URL * Monitoreo de logs * Herramientas de investigación de logs * Debugging * Captura de paquetes.	Los NGFws de palo alto permiten la gestion completa de sus dispositivos https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/firewall-administration	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Introduction.htm Pagina 17 del link Pagina 121 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
123	Consola de administración y monitoreo	Debe permitir la validación de las políticas, avisando cuando haya reglas que ofusquen o tengan conflicto con otras (shadowing)	La consola de administración y monitoreo de los NGFW de Palo Alto Networks permite validar las políticas de seguridad, detectando conflictos o reglas que se superpongan (shadowing), y alertando al administrador para evitar inconsistencias en la aplicación de las políticas. https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices/security-policy-best-practices/deploy-security-policy-best-practices/security-policy-rulebase-best-practices	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Network-Security-for-IoT-Devices.htm?Highlight=shadowing Pagina 457 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 93	No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
124	Consola de administración y monitoreo	Debe posibilitar la visualización y comparación de configuraciones actuales, la configuración anterior y configuraciones más antiguas (Control de versiones).	La consola de administración y monitoreo de los NGFW de Palo Alto Networks permite visualizar y comparar configuraciones actuales, anteriores y más antiguas, ofreciendo control de versiones que facilita auditorías, restauraciones y seguimiento de cambios en la política de seguridad. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/firewall-administration/manage-configuration-backups/perform-a-config-audit	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Log-Exporter-Advanced-Configuration-Parameters.htm?Highlight=Version%20control Pagina 256 - 266 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 116	No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
125	Consola de administración y monitoreo	Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó, IP de acceso, el horario del cambio, entre otros.	La consola de administracion permite reqlizar auditoria de cambios realizados https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/config-logs	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Log-Exporter-Advanced-Configuration-Parameters.htm?Highlight=Version%20control Pagina 25, 26, 83 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 132	No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
126	Consola de administración y monitoreo	Debe permitir la generación de mapas geográficos en tiempo real para la visualización de orígenes y destinos del tráfico generado en la Universidad.	Dentro de las capacidades del ACC (Application Command center) se ecnuebtra diferentes widgets y dashboards interactivos que muestran informacion grafica con los destinos y orígenes de todo el trafico generado https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/monitoring/use-the-application-command-center/widget-descriptions	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Log-Exporter-Advanced-Configuration-Parameters.htm?Highlight=Version%20control Pagina 196 del link	NO CUMPLE	En el link no brinda la información solicitada	No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
127	Consola de administración y monitoreo	Debe proveer resúmenes con la vista correlacionada de aplicaciones, amenazas (IPS, Anti Spyware) URLs y filtro de archivos, para un mejor diagnóstico y respuesta a incidentes.	dentro del ACC se correlacionan las entradas de logs y se resumen en widgets y dashboards interactivos para permitir tomar decisiones sobre el comportamiento de los usuarios	CUMPLE	La información se encuentra en el link proporcionado en el ítem 126	https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_LoggingAndMonitoring_AdminGuide/Topics-LMG/SmartEvent-Correlation-Unit.htm Pagina 99 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
128	Consola de administración y monitoreo	Debe ser posible acceder remotamente al sistema a aplicar configuraciones durante momentos donde el tráfico sea muy alto y la CPU y memoria del equipamiento este siendo totalmente utilizada.	Los NGFW de Palo alto Poseen la capacidad de acceder remotamente al sistema para Administracion y monitorear sin ningun problema gracias a la separacion de los planos de datos y de administracion, permitiendo que en el momento en que el plano de datos que analiza el trafico en su uso al 100% de su capacidad sea posible su acceso y gestion.	CUMPLE	La información se encuentra en el link proporcionado en el ítem 121	Se ofrecen varias formas de acceso remoto para administración y configuración: - SmartConsole *Aplicación gráfica para administración centralizada, configuración de políticas, monitoreo y actualizaciones. * Permite gestionar el gateway desde cualquier ubicación remota. https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_SecurityManagement_AdminGuide/Content/Topics-SECMG/SmartConsole-Window.htm?tocpath=Understanding%20SmartConsole%7C_____1 Pagina: 36 del link Check Point proporciona herramientas como: cpview: para monitoreo en tiempo real de CPU, memoria, tráfico y procesos. SmartView Monitor: para visualización gráfica del rendimiento. SNMP y API: para monitoreo externo y automatización. Estas herramientas permiten identificar cuellos de botella y aplicar cambios sin necesidad de reiniciar o interrumpir el servicio https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_SecurityManagement_AdminGuide/Content/Topics-SECMG/CLI/cpstat.htm?Highlight=CPU Pagina: 220 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
129	Consola de administración y monitoreo	Debe tener presentaciones de las siguientes informaciones, de forma histórica y en tiempo real (actualizado de forma automática y continua cada 1 minuto): * Debe mostrar la situación del dispositivo y del clúster. * Debe mostrar la versión actual del sistema y componentes. * Debe poder mostrar las principales aplicaciones. * Debe poder mostrar las principales aplicaciones por riesgo. * Debe poder mostrar los administradores autenticados en la plataforma de seguridad. * Debe poder mostrar el número de sesiones simultáneas * Debe poder mostrar el estado de las interfaces. * Debe poder mostrar el uso de CPU.	La consola de administración y monitoreo de los NGFW de Palo Alto Networks ofrece paneles en tiempo real e históricos, actualizados automáticamente cada minuto, que permiten visualizar: estado del dispositivo y clúster, versión del sistema y componentes, principales aplicaciones y por nivel de riesgo, administradores autenticados, número de sesiones simultáneas, estado de interfaces y uso de CPU, facilitando un monitoreo completo y continuo de la infraestructura. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring	CUMPLE		https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_LoggingAndMonitoring_AdminGuide/Topics-LMG/Monitoring-and-Handling-Alerts.htm?Highlight=real-time Pagina: 137 - 140 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
130	Reportes	Informe de uso de aplicaciones por usuario o por grupo de usuario.	Los NGFW de Palo Alto Networks permiten generar reportes detallados de uso de aplicaciones por usuario o grupo de usuarios, facilitando la visibilidad del tráfico, análisis de comportamiento y soporte para auditorías de seguridad.El acc como reportes personalizados permiten observar esta informacion https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/monitor/monitor-reports https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/acc/acc-tabs#idb3e5abb8-cadb-4b42-ab3b-6ab366cdb63c	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Creating-Application-Control-and-URL-Filtering-Rules.htm?Highlight=Report%20on%20application Pagina 288 - 295 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 132	No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
131	Reportes	Informes de actividad de usuario o grupo de usuarios, en donde se evidencie sitios visitados junto el tiempo de navegación.	Los NGFW de Palo Alto Networks permiten generar reportes detallados de actividades realizadas por usuarios a sitios visitadios usuario o grupo de usuarios, facilitando la visibilidad del tráfico, análisis de comportamiento y soporte para auditorías de seguridad.los reportes personalizados permiten observar esta informacion y las plantillas de ellos, tambien se evidencia en ACC en actividad de red https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/monitor/monitor-reports	CUMPLE		https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Reports.htm Pagina 55 del link	CUMPLE	La información se encuentra en el link proporcionado en el ítem 132	No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
132	Reportes	Informes por categorías, como, por ejemplo: Trafico, Amenazas, Filtrado red, amenazas y tendencias.	Los NGFW de palo alto en su ACC permiten dar visibilidad de la actividad de amenazas de red evidenciadas https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/acc/acc-tabs#idb3e5abb8-cadb-4b42-ab3b-6ab366cdb63c	CUMPLE		https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_Multi-DomainSecurityManagement_AdminGuide/CP_R81.20_MultiDomainSecurityManagement_AdminGuide.pdf Pagina: 125 del link https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_LoggingAndMonitoring_AdminGuide/CP_R81.20_LoggingAndMonitoring_AdminGuide.pdf Pagina 68 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta
133	Reportes	El Dashboard deben contener reportería con marcaciones de tendencia, es decir, información relevante que ayude a identificar comportamientos en la red.	El acc permite observar el comportamiento del trafico a traves de periodos de tiempo garantizacion la visualizacion de variaciones en el comportamiento usual	CUMPLE	La información se encuentra en el link proporcionado en el ítem 126	https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Views-and-reports.htm?tocpath=Views%20and%20Reports%7C_____0 Pagina: 59 del link	CUMPLE		No se diligencio el Item	NO CUMPLE	No se encuentra información que permita validar el cumplimiento en la documentación adjunta

ITEM	CARACTERÍSTICA TÉCNICA	DESCRIPCIÓN	GRUPO MICROSISTEMAS COLOMBIA S.A.S.			UNIÓN TEMPORAL UNIÓN TEMPORAL GESTIÓN INTEGRAL UD SEGURIDAD 2025			CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S.		
			UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
134	Documentación	Certificación vigente, suscrita directamente por el fabricante donde conste que la empresa oferente está certificada para brindar servicios y distribución autorizada por el tiempo de vigencia de la cotización y de ejecución del contrato	Pag. 138 del documento "propuesta gms proceso 009-2025.pdf"	CUMPLE		Pag. 385 y 388 del documento "OFERTA UT GESTION INTEGRAL UD SEGURIDAD 2025.pdf"	CUMPLE		Pag. 1-2 del documento "CERTIF~2.pdf" ubicado en la carpeta Parte 1	CUMPLE	
135	Documentación	Documento corporativo de fabrica en donde se encuentra la descripción detallada de las características de los equipos adquiridos y del licenciamiento aquí solicitado, en español o inglés.	Se adjunta la hoja de datos https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series	CUMPLE		Pag. 389-395 del documento "OFERTA UT GESTION INTEGRAL UD SEGURIDAD 2025.pdf"	CUMPLE		Pag. 1-10 del documento "secure-firewall-3100-series-ds.pdf" ubicado en la carpeta Parte 3	CUMPLE	
136	Documentación	Certificación vigente, suscrita directamente por el fabricante, en la cual conste que otorgará garantía durante el término que se encuentren vigente el licenciamiento.	Pag. 138 del documento "propuesta gms proceso 009-2025.pdf"	CUMPLE		Pag. 387 del documento "OFERTA UT GESTION INTEGRAL UD SEGURIDAD 2025.pdf"	CUMPLE		Pag. 1 del documento "LETTER~1.pdf" ubicado en la carpeta Parte 1	CUMPLE	
137	Documentación	Certificación expedida por la casa matriz donde se indica que es canal Partner en alguno de los niveles superiores de certificación según la marca, teniendo en cuenta que en orden ascendente los niveles de certificación son: Select, Advanced o Expert / Professional, Premier o Elite / Innovator, Platinum o Diamond / Premier, Gold o Platinum / o el equivalente a la marca.	Pag. 138 del documento "propuesta gms proceso 009-2025.pdf"	CUMPLE		Pag. 385 y 388 del documento "OFERTA UT GESTION INTEGRAL UD SEGURIDAD 2025.pdf"	CUMPLE		Pag. 1-2 del documento "CERTIF~2.pdf" ubicado en la carpeta Parte 1	CUMPLE	
138	Documentación	Certificación expedida por el fabricante de la marca ofertada, indicando que los equipos y componentes ofertados no se encuentran en periodo de fin de venta, y que mínimo tienen un ciclo de vida útil no inferior a cinco (5) años.	Pag. 138 del documento "propuesta gms proceso 009-2025.pdf"	CUMPLE		Pag. 386 del documento "OFERTA UT GESTION INTEGRAL UD SEGURIDAD 2025.pdf"	CUMPLE		Pag. 1 del documento "LETTER~1.pdf" ubicado en la carpeta Parte 1	CUMPLE	
139	Documentación	Carta de presentación de propuesta firmada por el representante legal (Anexo 1 de los estudios previos)	Pag. 3 del documento "propuesta gms proceso 009-2025.pdf"	CUMPLE		Pag. 1-2 del documento "OFERTA UT GESTION INTEGRAL UD SEGURIDAD 2025.pdf"	CUMPLE		Pag. 1 del documento "Carta de presentacionF.pdf" ubicado en la carpeta Parte 2	CUMPLE	
140	Documentación	Certificaciones de experiencia (Anexo 2 de los estudios previos)	Pag. 132 del documento "propuesta gms proceso 009-2025.pdf"	CUMPLE		Pag. 355 del documento "OFERTA UT GESTION INTEGRAL UD SEGURIDAD 2025.pdf"	CUMPLE		Pag. 1-2 del documento "Cert experienciaF.pdf" ubicado en la carpeta Parte 2	NO CUMPLE	El oferente envia el documento "Cert experienciaF.pdf" sin embargo, no envia certificados de experiencia y el RUP.
141	Documentación	Propuesta Económica (Anexo 3 de los estudios previos)	Pag. 192-793 del documento "propuesta gms proceso 009-2025.pdf"	CUMPLE		Pag. 1575-1576 del documento "OFERTA UT GESTION INTEGRAL UD SEGURIDAD 2025.pdf"	CUMPLE		Pag. 1 del documento "Oferta economica.pdf" ubicado en la carpeta Parte 1	CUMPLE	
EVALUACIÓN TÉCNICA			**HABILITADA**			**NO HABILITADA**			**NO HABILITADA**		

	NOMBRE	CARGO	FIRMA	FECHA
Responsable de la elaboración técnica	**Santiago Lopez Gomez**	**CPS Red de Datos UDNET - Area de Plataformas computacionales**	Santiago Lopez	23/08/2024
Aprobó	**Yuleima Ortiz Zambrano**	**Lider Red de Datos UDNET**		23/08/2024