UNIVERSIDAD NACIONAL DE PIURA
SECRETARÍA GENERAL

RESOLUCIÓN RECTORAL N° 0729-R-2024
Piura, 26 de setiembre del 2024

VISTO:

El expediente N° **000034-6202-24-8** presentado por la **Dra. Ing. Jassayra Araliz Chulle Chapilliquen**, Jefa de la Oficina de Tecnologías de la Información de la Universidad Nacional de Piura, que contiene el Informe N° 063-2024-OTI-UNP del 16.Set.2024, el Informe N° 1262-2024-OCAJ-UNP del 23.Set.2024, el Oficio N° 2187-R-UNP-2024 del 26.Set.2024, y;

CONSIDERANDO:

Que, de conformidad con el artículo 18° de la Constitución Política del Perú, prescribe: *"(…) Cada universidad es autónoma en su régimen normativo, de gobierno, académico, administrativo y económico. Las universidades se rigen por sus propios estatutos en el marco de la Constitución y de las leyes (…)";*

Que, mediante Ley N° 13531 del 03.Mar.1961, fue creada la Universidad Nacional de Piura, cuya sede está ubicada en el Distrito de Castilla, Departamento de Piura, cuyos fines se encuentran estipulados en el Artículo 8° del Estatuto de la Universidad Nacional de Piura, Aprobado en Sesión Plenaria de Asamblea Estatutaria del 13.Oct.2014 (Ley N° 30220 - Ley Universitaria);

Que, el Artículo 8° de la Ley Universitaria – Ley N° 30220, prescribe: *"(…) La autonomía inherente a las universidades se ejerce de conformidad con lo establecido en la Constitución, la presente Ley y demás normativa aplicable. Esta autonomía se manifiesta en los siguientes regímenes: (…) académico, económico y administrativo"*;

Que, el numeral 29.4 del artículo 29° del Reglamento de la Ley de Contrataciones del Estado, aprobado por Decreto Supremo N° 344-2018-EF, señala que en la definición del requerimiento no se hace referencia a fabricación o procedencia, procedimiento de fabricación, marcas, patentes o tipos, origen o producción determinados, ni descripción que oriente la contratación hacia ellos, salvo que la Entidad haya implementado el correspondiente proceso de estandarización debidamente autorizado por su Titular, en cuyo caso deben agregarse las palabras "o equivalente" a continuación de dicha referencia.

Que, mediante Resolución N° 011-2016-OSCE/PRE se aprueba la Directiva N° 004-2016- OSCE/CD "Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular", la cual establece en su numeral 6.1 que **la estandarización es el proceso de racionalización consistente en ajustar a un determinado tipo o modelo los bienes o servicios a contratar, en atención a los equipamientos preexistentes**;

Que, según lo establecido en el numeral 7.2 de la citada Directiva los presupuestos que deben verificarse para que proceda la estandarización, son los siguientes: a. La Entidad posee determinado equipamiento o infraestructura, pudiendo ser maquinarias, equipos, vehículos u otro tipo de bienes, así como ciertos servicios especializados, b. Los bienes o servicios que se requieren contratar son accesorios o complementarios al equipamiento o infraestructura preexistente e imprescindibles para garantizar la funcionalidad, operatividad o valor económico del equipamiento o infraestructura;

RESOLUCIÓN RECTORAL N° 0729-R-2024
Piura, 26 de setiembre del 2024

Que, el numeral 7.3 de la Directiva en mención señala que el área usuaria elabora un informe técnico de estandarización debidamente sustentado, el cual contendrá como mínimo: a. La descripción del equipamiento o infraestructura preexistente de la entidad; b. De ser el caso, la descripción del bien o servicio requerido, indicándose la marca o tipo de producto; así como las especificaciones técnicas o términos de referencia, según corresponda; c. El uso o aplicación que se le dará al bien o servicio requerido; d. La justificación de la estandarización, donde se describa objetivamente los aspectos técnicos, la verificación de los presupuestos para la estandarización antes señalados y la incidencia económica de la contratación; e. Nombre, cargo y firma de la persona responsable de la evaluación que sustenta la estandarización del bien o servicio, y del jefe del área usuaria; f. La fecha de elaboración del informe técnico;

Que, en ese sentido, mediante Informe N° 063-2024-OTI-UNP del 16.Set.2024, la Dra. Ing. Jassayra Araliz Chulle Chapilliquen, Jefa de la Oficina de Tecnologías de la Información de la Universidad Nacional de Piura, se dirige ante el señor Rector para solicitarle la estandarización del equipamiento de tecnologías, según se detalla:

- Switches y access point, con la marca CISCO SYSTEMS.
- Servidores de Procesamiento y Almacenamiento, con la marca Hewlett Packard Enterprise - HPE.
- Firewalls de nueva generación, Licencias de Protección de CIBERSEGURIDAD para correo de nube, Licencias de Protección con firewall virtuales para máquinas virtuales de nube, Licencias de Protección lateral: XDR, NDR; con la marca CHECK POINT.

Informando que las plataformas de los equipos indicados con las que cuenta actualmente la UNP, corresponden en su totalidad con las marcas indicadas, según se detalla:

- Para los switches y access point, actualmente corresponde al 97% del equipamiento existente a la marca CISCO SYSTEMS.
- Para los Servidores de Procesamiento y Almacenamiento, actualmente corresponde al 100% del equipamiento existente a la marca Hewlett Packard Enterprise – HPE
- Para los Firewalls de nueva generación, actualmente corresponde al 100% del equipamiento existente a la marca CHECK POINT.

Asimismo, informa que el máximo desempeño en la gestión de la red, todos los equipos centrales CORE de la UNP corresponden a las marcas CISCO SYSTEMS, HPE, CHECK POINT, las cuales están configurados protocolos avanzados; con lo cual estamos optimizando la operación de la red de datos, el procesamiento de las aplicaciones y el almacenamiento de la base de datos de manera segura, por lo tanto, se solicita que los nuevos equipos que sean comprados con las marcas descritas, en cada sistema. Adjuntando el informe, donde se detallan los aspectos técnicos de operación actual, que sustentan la solicitud de estandarización -Anexo 1, 2 y 3-;

Que, con Informe N° 1262-2024-OCAJ-UNP del 23.Set.2024, la Dra. Norma A. Ramírez Dioses, Jefa (e) de la Oficina Central de Asesoría Jurídica señala textualmente lo siguiente:

*"**BASE LEGAL Y ANALISIS**:*

2.1. El Artículo 16° del TUO de la Ley N° 30225, Ley de Contrataciones del Estado, establece: 16° Requerimiento. - 16.1 El área usuaria requiere los bienes, servicios u obras a contratar, siendo responsable de formular las especificaciones técnicas,

términos de referencia o expediente técnico, respectivamente, así como los requisitos de calificación, además de justificar la finalidad pública de la contratación. Los bienes, servicios u obras que se requieran deben estar orientados al cumplimiento de las funciones de la Entidad. 16.2 Las especificaciones técnicas, términos de referencia a expediente técnico deben formularse de forma objetiva y precisa por el área usuaria, alternativamente pueden ser formulados por el órgano a cargo de las contrataciones y aprobados por el área usuaria Dichas especificaciones técnicas, términos de referencia o expediente técnico deben proporcionar acceso al proceso de contratación en condiciones de igualdad y no tienen por efecto la creación de obstáculos ni direccionamiento que perjudiquen la competencia en el mismo. Salvo las excepciones previstas en el reglamento, en el requerimiento no se hace referencia a una fabricación o una procedencia determinada, o a un procedimiento concreto que caracterice a los bienes o servicios ofrecidos por un proveedor determinado, o a marcas, patentes o tipos, o a un origen o a una producción determinados con la finalidad de favorecer o descartar ciertos proveedores o ciertos productos (Subrayado y resaltado es agregado).

2.2. Por su lado en la Opinión N° 176-2018/DTN, de fecha 23 de octubre de 2018, la Dirección Técnica Normativa del Organismo Supervisor de las Contrataciones del Estado-OSCE, ha señalado: (…) 2.1. En primer lugar, debe indicarse que el área usuaria requiere los bienes, servicios u obras a contratar, siendo responsable de formular las especificaciones técnicas, términos de referencia o expediente técnico, respectivamente, además de justificar la finalidad pública de la contratación, en esa medida, debe tenerse en cuenta que los bienes, servicios u obras que se requieran deben estar orientados al cumplimiento de las funciones de la Entidad. En esa línea, el numeral 16.2 del artículo 16° de la Ley señala que "Las especificaciones técnicas, términos de referencia o expediente técnico deben formularse de forma objetiva y precisa por el área usuaria, alternativamente pueden ser formulados por el órgano a cargo de las contrataciones y aprobados por el área usuaria. Dichas especificaciones técnicas, términos de referencia o expediente técnico deben proporcionar acceso al proceso de contratación en condiciones de igualdad y no tienen por efecto la creación de obstáculos ni direccionamiento que perjudiquen la competencia en el mismo. Salvo las excepciones previstas en el reglamento en el requerimiento no se hace referencia a una fabricación o una procedencia determinada, o a un procedimiento concreto que caracterice a los bienes o servicios ofrecidos por un proveedor determinado, o a marcas, patentes o tipos, o a un origen o a una producción determinados con la finalidad de favorecer o descartar ciertos proveedores o ciertos productos. Por su parte, el numeral 84 del artículo 8° del Reglamento dispone que "En la definición del requerimiento no se hace referencia a fabricación o procedencia, procedimiento de fabricación, marcas, patentes o tipos, origen o producción determinados, ni descripción que oriente la contratación hacia ellos, salvo que la Entidad haya implementado el correspondiente proceso de estandarización debidamente autorizado por su Titular, en cuyo caso deben agregarse las palabras "o equivalente" a continuación de dicha referencia (...)" Como se aprecia, la normativa de contrataciones del Estado establece que las Entidades no pueden hacer referencia a marcas cuando formulen sus requerimientos de bienes, servicios u obras, de esta manera, el requerimiento debe ser efectuado de forma genérica, sin consignar marcas que ***orienten la contratación hacia un proveedor en particular****. 2.2. No obstante, lo antes señalado, si bien la prohibición de hacer referencia a marcas constituye la regla general que deben observar las Entidades al momento de elaborar sus requerimientos para la contratación de obras, existen casos como el mejoramiento, renovación o ampliación, entre otros- en los que la inclusión de marcas en el expediente técnico podría resultar necesaria a efectos de no afectar los sistemas*

que vienen funcionando (sistemas contra incendios, sistemas de aire acondicionado, etc.) y/o los procesos que se vienen desarrollando (procesos de tratamiento de agua, a manera de ejemplo) en la obra preexistente. Así, de manera excepcional, podría hacerse referencia a marcas en un expediente técnico de obra, siempre que ello resulte indispensable para alcanzar la finalidad de la contratación y en la medida que no se afecte la libre concurrencia de proveedores bajo ninguna circunstancia. 3. CONCLUSIONES: 3.1 La normativa de contrataciones del Estado establece que las Entidades no pueden hacer referencia a marcas cuando formulen sus requerimientos de bienes, servicios u obras, de esta manera, el requerimiento debe ser efectuado de forma genérica, sin consignar marcas que orienten la contratación hacia un proveedor en particular. 3.2. Si bien la prohibición de hacer referencia a marcas constituye la regla general que deben observar las Entidades al momento de elaborar sus requerimientos para la contratación de obras, existen casos - como el mejoramiento, renovación o ampliación, entre otros- en los que la inclusión de marcas en el expediente técnico podría resultar necesaria a efectos de no afectar los sistemas que vienen funcionando (sistemas contra incendios, sistemas de aire acondicionado, etc.) y/o los procesos que se vienen desarrollando (procesos de tratamiento de agua, a manera de ejemplo) en la obra preexistente. Así, de manera excepcional, podría hacerse referencia a marcas en un expediente técnico de obra, siempre que ello resulte indispensable para alcanzar la finalidad de la contratación y en la medida que no se afecte la libre concurrencia de proveedores bajo ninguna circunstancia..." (…)

***CONCLUSIONES**:*

a. Que, al respecto se tiene que mediante el Informe N° 063-2024-OTI-UNP, de fecha 16 de setiembre de 2024; la jefa de la Oficina de Tecnologías, solicita al Sr. Rector la estandarización del equipamiento de tecnologías, según el documento de su propósito, entendiendo que se refiere a los equipos que se pudieran adquirir por parte de la entidad en futuras compras por parte del Órgano Encargado de las Contrataciones, siendo que al respecto y tal como lo señala la normativa de contrataciones del Estado, esta nos señala que si bien las Entidades no pueden hacer referencia a marcas cuando formulen sus requerimientos de bienes, servicios u obras; de esta manera, el requerimiento debe ser efectuado de forma genérica, sin consignar marcas que orienten la contratación hacia un proveedor en particular, sin embargo, en atención al informe a la jefa de la Oficina de Tecnologías, resulta procedente aprobar el proceso de estandarización para las adquisiciones de equipos de red.";

Que, con Oficio N° 2187-R-UNP-2024 del 26.Set.2024, el CPC. Dr. Enrique Ramiro Cáceres Florián, Rector (e) de la Universidad Nacional de Piura, remite los actuados a la oficina de Secretaria General para la emisión de la resolución rectoral;

Que, la presente Resolución se suscribe en virtud al Principio de Legalidad, por el cual las autoridades administrativas deben actuar con respeto a la Constitución, la ley y al derecho, dentro de las facultades que le estén atribuidas y de acuerdo con los fines para los que les fueron conferidas; así como al Principio de Buena Fe Procedimental, por el cual la autoridad administrativa, los administrados, sus representantes o abogados y, en general, todos los partícipes del procedimiento, realizan sus respectivos actos procedimentales guiados por el respeto mutuo, la colaboración y la buena fe (…), previstos en el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General aprobado por Decreto Supremo N° 004-2019-JUS;

RESOLUCIÓN RECTORAL N° 0729-R-2024
Piura, 26 de setiembre del 2024

Que, de conformidad con el artículo 175º inciso 3) del Estatuto de la Universidad Nacional de Piura, que prescribe: *"El Rector es el representante legal de la Universidad y ejerce el gobierno de la misma (…)."* Señalando dentro de sus funciones, *"inciso 3) Dirigir la actividad académica de la Universidad y su gestión administrativa, económica y financiera."*;

Que, estando a lo dispuesto por el señor Rector (e), en uso de sus atribuciones legales conferidas, con visto de la Oficina de Tecnologías de la Información, la Oficina Central de Asesoría Jurídica y la Secretaria General;

SE RESUELVE:

ARTÍCULO 1°- APROBAR, el Proceso de Estandarización para el Equipamiento de Tecnologías, según lo establecido en el Informe N° 063-2024-OTI-UNP y sus Anexos 1, 2 y 3 que forman parte integrante de la presente Resolución.

ARTÍCULO 2°.- PRECISAR que la aprobación de la estandarización a que se refiere el artículo precedente, no implica exoneración del cumplimiento de los requisitos, condiciones, formalidades, exigencias y garantías establecidos por la Ley N° 30225, Ley de Contrataciones del Estado y sus modificatorias, así como su Reglamento y modificatorias, para la realización de los actos del procedimiento de selección que corresponda y la ejecución contractual respectiva.

ARTÍCULO 3°.- NOTIFICAR, a los órganos administrativos pertinentes de la Universidad Nacional de Piura.

REGÍSTRESE, COMUNÍQUESE Y EJECÚTESE.

ANEXO:
- Informe N° 063-2024-OTI-UNP y sus Anexos 1, 2 y 3

c.c.: RECTOR, DGA, URH, OTI, ABAST, UC, UP, UT, OPYPTO, ARCHIVO
10 copias/VAGV

Universidad Nacional de Piura
Secretaría General
Abg. Vanessa Arline Girón Viera
SECRETARIA GENERAL

UNIVERSIDAD NACIONAL DE PIURA
DR. ENRIQUE RAMIRO CÁCERES FLORIÁN
RECTOR (e)

ANEXO 1

UNIVERSIDAD NACIONAL DE PIURA

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

INFORME TÉCNICO N°001 PARA LA ESTANDARIZACIÓN DE EQUIPAMIENTO DE LA MARCA CISCO PARA LA RED SWITCH Y ACCESS POINT DE LA UNP

1. **Nombre de la Oficina**

   Oficina de Tecnología de la Información.

2. **Nombre y Cargo de los responsables de la Evaluación**

   Jassayra Araliz Chulle Chapilliquen
   Jefe de la Oficina de Tecnología de la Información

UNIVERSIDAD NACIONAL DE PIURA
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
RECIBIDO: 9 SEP 2024 HORA:
FOLIO N°

3. **Fecha**

   Piura, 09 de septiembre de 2024

4. **Objetivo**

   El presente documento tiene por finalidad, establecer el sustento técnico que permita mantener la operación de la solución de la red de datos de la universidad, con los niveles eficientes de comunicación y seguridad de red estable, para lo cual debe estar estandarizada en la institución, las adquisiciones de soluciones de equipamiento de red alámbrica e inalámbrica: switches y access point, correspondientes a la marca del equipamiento preexistente y que son mundialmente reconocidas por su confiabilidad, actualización continua a firmware, soporte técnico y continuidad de sus productos. Así mismo el equipamiento de red moderno de switch (core y de borde), wireless controller y access point, que fueron adquiridos por la UNP en el año 2021, cubren el 97% de la red de datos, las mismas que ya han caducado el soporte tecnico y garantia del contratista y de la marca, la cual configura un riego latente de falla en cualquier momento, y no se tenga activa la garantía de estos equipos para el reemplazo de piezas parcial o total, pero igualmente demostrando que la marca tiene una robustes de operación de forma consecutiva, resulta muy necesario activar los contratos de soporte y garantía con la marca CISCO SYSTEMS, y que la estandarización de la marca, permita las adquisiciones de nuevo equipamiento de red alámbrica e inalámbrica, comprendidas por equipos conmutadores de red (switch), controlador inalámbrico y access point, sean compatibles con la red existente.

5. **Marco Legal**

   5.1 El Numeral 29.4 del Artículo 29° del Reglamento de Contrataciones del Estado, establece que: *"... salvo que la Entidad haya implementado el correspondiente proceso de estandarización debidamente autorizado por su Titular, en cuyo caso se agregan las palabras "o equivalente" a continuación de dicha referencia"*.

   5.2 En el Anexo N° 1 del Reglamento de Contrataciones del Estado se define Estandarización como *"Proceso de racionalización consistente en ajustar a un determinado tipo o modelo los bienes o servicios a contratar, en atención a los equipamientos existentes."*

5.3 En tal sentido, y dado que la Directiva N°004-2016-OSCE/CD que refiere los Lineamientos para la Contratación en la que se hace Referencia a Determinada Marca o Tipo Particular de producto, indicando:

"Cuando en una contratación en particular el área usuaria - aquella de la cual proviene el requerimiento de contratar o que, dada su especialidad y funciones, canaliza los requerimientos formulados por otras dependencias - considere que resulta inevitable definir el requerimiento haciendo referencia a fabricación o procedencia, procedimiento de fabricación, marcas, patentes o tipos, origen o producción determinados o descripción que oriente la contratación hacia ellos, deberá elaborar un informe técnico de estandarización debidamente sustentado, el cual contendrá como mínimo:

a. La descripción del equipamiento o infraestructura preexistente de la entidad.
b. La descripción del bien o servicio requerido, indicándose la marca o tipo de producto; así como las especificaciones técnicas o términos de referencia, según corresponda.
c. El uso o aplicación que se le dará al bien o servicio requerido.
d. La justificación de la estandarización, donde se describa objetivamente los aspectos técnicos, la verificación de los presupuestos para la estandarización antes señalados y la incidencia económica de la contratación.
e. Nombre, cargo y firma de la persona responsable de la evaluación que sustenta la estandarización del bien o servicio, y del jefe del área usuaria.
f. La fecha de elaboración del informe técnico."

6. Descripción del Equipamiento o Infraestructura Preexistente

La UNIVERSIDAD NACIONAL DE PIURA, actualmente cuenta con el siguiente equipamiento de la marca CISCO en toda su red de datos:

- Equipamiento de conmutadores de red – SWITCH:
  - SWITCH TIPO CORE DE DATA CENTER, existente dos (02) equipos de la marca "CISCO" Serie Nexus 9300, modelo 93180, utilizados como equipos núcleo de la DMZ de la Universidad. Estos concentran toda la data de la universidad, permitiendo una conmutación de datos eficiente entre todos los equipos de red de distribución y borde de la universidad.
  - SWITCH TIPO CORE LAN, existente cuatro (04) equipos de la marca "CISCO" Series Catalyst 9500, modelo 9500-48Y4C-A, utilizados como equipos núcleo de la red LAN de la Universidad. Estos concentran toda la data de la universidad, permitiendo una conmutación de datos eficiente entre todos los equipos de red de distribución y borde de la universidad.
  - SWITCH TIPO BORDE, existen equipos de la marca "CISCO" de las series Catalyst 9200L, utilizados como equipos de distribución y borde en la red de la Universidad. Estos concentran el tráfico de la red de datos de todos los terminales de la Universidad, como son las laptops, desktop, cámaras IP, Access Point, control de accesos, etc, para ser enviados a los equipos de red nucleo (SWITCH CORE CISCO LAN 9500-48Y4C).
    A la fecha todos los equipos SWITCH están sin garantía y sin soporte de fábrica.
- Equipamiento de redes inalámbricas: a la fecha todos los equipos de la red inalámbrica están descontinuados y sin garantía y sin soporte de fábrica.

- CONTROLADOR INALÁMBRICO, existe un (01) equipo de la marca CISCO de la serie 9800, utilizado para gestionar, concentrar, analizar, procesar y filtrar el tipo de trafico de los equipos periféricos existentes Access Point de todo el campus, permitiendo la administración centralizada y eficiente de los equipos inalámbricos.

- ACCESS POINT INALÁMBRICOS, existen equipos de la marca CISCO de las series indoor: C9115AX y outdoor AIR-AP1562I-A-K9, utilizados en todo el campus para propagar señal WiFi a todo el campus para la conexión de los alumnos, docentes y administrativos. para sus actividades diarias

6.1. Equipamiento de conmutadores de red – SWITCH

Se detalla las características de los equipos SWITCH CORE que actualmente están operando:

Detalles Técnicos:		
Fabricante:	Cisco	
Tipo y categoría:	Hardware/Software switch	
Solución y modelo:	SWITCH TIPO CORE Cisco Nexus 93180YC	
Características:		
	Ports	48 x 1/10/25-Gbps and 6 x 40/100-Gbps QSFP28 ports
	CPU	4CORES
	System Memory	24 Gb
	SSD drive	64GB
	System buffer	40MB
	Management ports	2 ports; 1RJ-45 and 1SFP
	USB ports	1
	RS-232 serial ports	1
	Power supplies (up to 2)	500W AC, 650W AC, 930W DC, or 1200W HVAC/HVDC
	Fans	4
	Acoustics	48.5 dBA at 40% fan speed, 64,9 dBA at 70% fan speed, and 77,8 dBA at 100% fan speed
Características:		
Performance	Maximum number of Longest Prefix March (LPM) routes	896000
	Maximum number of IP host entries	896000
	Maximum number of MAC address entries	256000

	Maximum number of multicast routes	32000
	Number of Interior Gateway Management Protocol (IGMP) snooping groups	Shipping: 8000 Maximum: 32000
	Maximum number of Cisco Nexus 2000 Series Fabric Extenders per switch	16
	Maximum number of Access Control List (ACL) entries	Per slice of the forwarding engine: 4000 ingress 2000 egress Total (2 forwarding slices): 8000 ingress 4000 ingress
	Maximum number of VLANs	4096
	Number of Virtual Routing anf Forwarding (VRF) instances	Shipping: 1000 Maximum: 16000
	Maximum number of ECMP paths	64
	Maximum number of port channels	512
	Maximum number of links in a port channel	32
	Number of active SPAN sessions	4
	Maximum number of VLANs in Rapid per-VLAN Spanning Tree (RPVST) instances	3967
	Maximum number of Hot-Standby Router Protocol (HSRP) groups	490
	Number of Network Address Translation (NAT) entries	1023
	Maximum number of Multiple Spanning Tree (MST) instances	64
	Flow-table size used for Cisco Tetration Analytics platform	64000
	Number of Queues	8
Requisitos del sistema		
Plataforma:	Sistema operativo NX-OS (NXOS-7031 4.2)	
Soporte técnico	Equipo vigente en la marca.	

Se detalla las características de los equipos SWITCH CORE LAN DE CAMPUS que actualmente están operando:

UNIVERSIDAD NACIONAL DE PIURA

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

Detalles Técnicos:	
Fabricante:	Cisco
Tipo y categoría:	Hardware/Software switch
Solución y modelo:	SWITCH TIPO CORE LAN Cisco Catalyst C9500-48Y4C-A
Características:	
	▪ FACTOR DE FORMA: 1U RACKEABLE, CISCO. ▪ 48 PUERTOS DE 1/10/25G GIGABIT ETHERNET Y 4 PUERTOS 40G QSFP. ▪ CADA SWITCH CONTEMPLA 04 TRANSCEIVER PARA TRANSMISION A 40G, POR CADA EQUIPO HABILITADO, Y SOPORTA A FUTURO VELOCIDADES DE 100G. ▪ CON FUENTE REDUNDANTE. ▪ MEMORIA DRAM 16GB Y FLASH 16GB.
Características:	
Performance	▪ NUMERO DE DIRECCIONES MAC: 82000 ▪ TOTAL DE RUTAS IPV4 DE HOST: 90000 ▪ TOTAL DE RUTAS IPV6 DE HOST: 90000 ▪ TOTAL DE RUTAS MULTICAST IPV4: 32000 ▪ TOTAL DE RUTAS MULTICAST IPV6: 32000 ▪ ESCALA QOS ACL: 16000 ▪ ESCALA ACL SECURITY: 16000 ▪ ENTRADAS DE FNF 98000 ▪ ID DE VLANS: 4000 ▪ INTERFACE VIRTUALES CONMUTADAS: 1000 ▪ CAPACIDAD DE CONMUTACIÓN: 3.2 TBPS ▪ FORWARDING RATE: 1 BPPS
Características:	
Standards	▪ SOPORTAR PROTOCOLOS CAPA 2: 802.1S, 802.1W, 802.1P, 802.1X (Y REV), 802.3AD, 802.1Q, 802.1D, PVLAN, VRRP, PBR, CDP, QOS. ▪ SOPORTAR EN GESTION: RMON I, II STANDARDS SNMPV1, SNMPV2C, AND SNMPV3. ▪ SOPORTAR PROTOCOLOS CAPA 3: EIGRP, HSRP, OSPF, VXLAN, BGP. ▪ SOPORTAR AUTOMATIZACION: NETCONFIG, YANG, PNP. ▪ SOPORTAR SEGURIDAD MAC SEC 128 Y 256.
Requisitos del sistema	
Plataforma:	Sistema operativo Cisco IOS
Soporte	
Soporte técnico	Equipo vigente en la marca.

Se detalla las características de los equipos SWITCH DE BORDE que actualmente están operando:

Detalles Técnicos:	
Fabricante:	Cisco
Tipo y categoría:	Hardware/Software switch
Solución y modelo:	SWITCH TIPO BORDE Cisco Catalys 9200L Advantage C9200L-48P-4X-A C9200L-48T-4X-A

	C9200L-24P-4X-A C9200L-24T-4X-A
Características:	
	24 and 48 ports of Gigabit Ethernet (GbE) 10/100/1000 desktop connectivity
Características:	
Performance	▪ Factor de forma: 1U Rackeable, CISCO ▪ Memoria DRAM 2GB / Flash 4GB ▪ Paquete de buffer: 6 MB ▪ Debe tener modulo stack dedicado con staking bandwitch de minimo 80Gbps. ▪ Numero de direcciones MAC: 16000 ▪ Entradas de enrutamiento IPv4: 3000 ▪ Entradas de enrutamiento IPv6: 1500 ▪ Escala de enrutamiento Multicast: 1000 ▪ Entradas de escala QoS: 1000 ▪ Entradas de escala ACL: 1500 ▪ Entradas de FNF 16,000 ▪ ID de VLANs: 4090 ▪ Interface Virtuales Conmutadas: 512 ▪ Capacidad de conmutación: 176 Gbps (C9200L-48P-4X-A, C9200L-48T-4X-A), 128 Gbps (C9200L-24P-4X-A, C9200L-24T-4X-A) ▪ Forwarding Rate: 130 Mpps (C9200L-48P-4X-A, C9200L-48T-4X-A), 95 Mpps (C9200L-24P-4X-A, C9200L-24T-4X-A)
Características:	
Standards	▪ soportar protocolos capa 2: 802.1s, 802.1w, 802.1p, 802.1x, 802.3ad, 802.1Q, PVLAN, VRRP, PBR, CDP, QoS. ▪ Soportar protocolos capa 3: RIP, EIGRP Stub, OSPF 1000 routes. ▪ Soportar automatizacion: NETCONFIG, YANG, PnP. ▪ Soportar seguridad MAC SEC 128.
Requisitos del sistema	
Plataforma:	Sistema operativo Cisco IOS
Soporte	
Soporte técnico	Equipo vigente en la marca.

6.2. Equipamiento de redes inalámbricas

Se detalla las características de los equipos CONTROLADOR INALAMBRICO que actualmente están operando:

Detalles Técnicos:	
Fabricante:	Cisco
Tipo y categoría:	Hardware/Software Wireless LAN Controller
Solución y modelo:	Cisco C9800-40-K9
Características:	

Componentes:	▪ Factor de forma: 1U Rackeable, CISCO. ▪ con 4 puertos de 1/10G SFP+ ▪ con fuente redundante. ▪ Del tipo Red definida por el usuario. ▪ Soportar actualización de imagen completa y una actualización mientras la red aún está funcionando. ▪ Soportar throughput Mínimo: 40 Gbps. ▪ Soportar minimo: 1900 access point. ▪ Soportar minimo: 31000 clientes. ▪ Soportar WLAN minimo: 4090 ▪ Soportar VLAN minimo: 4090 ▪ Soportar policy tags: 2000. ▪ Soportar en seguridad: ETA, image signing, secure boot, MACsec encryption, WIPS, WPA2, WPA3, TSL, Encapsulating Security Payload (ESP) Triple DES (3DES) Transform. ▪ Soportar estandares wireless: IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11n, 802.11k, 802.11r, 802.11u, 802.11w, 802.11ac Wave1 and Wave2, 802.11ax. ▪ Soportar estandares y switching: IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, 1000BASE-T. 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q VLAN tagging, 802.1AX Link Aggregation. ▪ Soportar emcriptacion: AES, CBC-MAC, DES, 3DES, DTLS, IPSEC, MACSEC. ▪ Soportar en gestion: RMON, SNMPv1, SNMPv2c, and SNMPv3. ▪ Soportar protocolos capa 3: EIGRP, HSRP, OSPF, VXLAN, BGP. ▪ Soportar visibilidad de telemetria. Soportar automatizacion: NETCONFIG, YANG, PnP.
Soporte	
Soporte técnico	Equipo vigente en la marca.

Se detalla las características de los equipos Access Point Indoor que actualmente están operando:

Detalles Técnicos:	
Fabricante:	Cisco
Tipo y categoría:	Hardware/Software Access Point Indoor
Solución y modelo:	Cisco Catalyst Series C9115AXI-A
Características:	
Componentes:	▪ Access point con antenas integradas CISCO ▪ Antena intena integrada con ganancia de 3dBi para 2.4Ghz. ▪ Antena intena integrada con ganancia de 4dBi para 5Ghz. ▪ Soportar interfaces de: un puerto 100, 1000, 2500 Multigigabit Ethernet (RJ-45) IEEE 802.3bz, un puerto Management console (RJ-45), y un puerto USB. ▪ Memoria DRAM 2048 GB y Flash 1024 GB. ▪ Soportar estandares wireless: IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac Wave1 and Wave2, 802.11ax. ▪ Soportar Bluetooth 5.0

	▪ En seguridad soportar: 802.11i, WPA3, WPA2, WPA, 802.1X, Advanced Encryption Standard (AES). ▪ Soportar estandares: IEEE 802.3, IEEE 802.3ab, IEEE 802.3af/at ▪ Soportar Extensible Authentication Protocol (EAP). ▪ Soportar para conexiones por 802.11n: ✓ 4x4 MIMO ✓ Maximal Ratio Combining (MRC) ✓ 802.11n and 802.11a/g beamforming ✓ Canales 20, y 40 MHz ✓ PHY data rates up to 890 Mbps (40 MHz with 5 GHz and 20 MHz with 2.4 GHz) ✓ A-MPDU (transmit and receive), A-MSDU (transmit and receive) ✓ Dynamic Frequency Selection (DFS) ✓ Cyclic Shift Diversity (CSD) support ▪ Soportar para conexiones por 802.11ac: ✓ 4x4 downlink MU-MIMO ✓ 802.11ac beamforming ✓ Canales 20, 40, 80 y 160 MHz ✓ PHY data rates up to 3.47 Gbps (160 MHz with 5 GHz) ✓ Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive) ✓ MRC, DFS, y CSD ▪ Soportar para conexiones por 802.11ax: ✓ 4x4 downlink MU-MIMO ✓ Uplink/downlink OFDMA ✓ DFS, CSD, TWT, BSS coloring, MRC, beamforming ✓ Canales 20, 40, 80 y 160 MHz ✓ PHY data rates up to 5.38 Gbps (160 MHz with 5 GHz and 20 MHz with 2.4 GHz) ✓ Packet aggregation: A-MPDU, A-MSDU
Soporte	
Soporte técnico	Equipo vigente en la marca.

Se detalla las características de los equipos Access Point Outdoor que actualmente están operando:

Detalles Técnicos:	
Fabricante:	Cisco
Tipo y categoría:	Hardware/Software Access Point Outdoor
Solución y modelo:	Cisco Catalyst Series AIR-AP1562I-A-K9
Características:	
Componentes:	▪ Access point con antenas integradas CISCO ▪ Antena intena integrada con ganancia de 7dBi para 2.4Ghz. ▪ Antena intena integrada con ganancia de 4dBi para 5Ghz. ▪ Soportar interfaces de: 100, 1000 Ethernet (RJ-45), un puerto Management console (RJ-45), y un puerto SFP. ▪ Soportar estandares wireless: IEEE 802.11a/g/n/ac, Wave 2. ▪ En seguridad soportar: 802.11i, WPA2, WPA, 802.1X, Advanced Encryption Standard (AES).

	▪ Soportar estandares: IEEE 802.3at ▪ Soportar Extensible Authentication Protocol (EAP). ▪ Coexistencia 4G LTE. ▪ Soportar para conexiones por 802.11n: ✓ 3 x 3 MIMO with three spatial streams ✓ MRC ✓ Canales 20, y 40 MHz ✓ PHY data rates up to 450 Mbps ✓ Packet aggregation: A-MPDU (Tx/Rx) and A-MSDU (Tx/Rx) ✓ Opcional soportar Dynamic Frequency Selection (DFS) y Cyclic-Shift-Diversity (CSD)[1] ▪ Soportar para conexiones por 802.11ac: ✓ 3 x 3 MIMO with three spatial streams ✓ Multi- and single-user MIMO ✓ Maximal Ratio Combining (MRC) ✓ 802.11ac beamforming (transmit beamforming) ✓ Canales 20, 40, y 80 MHz ✓ PHY data rates up to 1.3 Gbps (80 MHz in 5 GHz) ✓ Packet aggregation: A-MPDU (Tx/Rx) and A-MSDU (Tx/Rx) ✓ Dynamic Frequency Selection (DFS) y Cyclic-Shift-Diversity (CSD)
Soporte	
Soporte técnico	Equipo vigente en la marca.

7. Descripción del Bien a Estandarizar

El presente documento tiene por finalidad, establecer el sustento para la estandarización la renovación del equipamiento de red alámbrica e inalámbrica, con la marca CISCO SYSTEMS.

La renovación del equipamiento con la marca CISCO es imprescindible para garantizar la operatividad eficiente de la solución de la red de datos de la universidad, ya que actualmente los switch operan con el protocolo EIGRP propietario de la marca, la cual ha demostrado una eficiente operación.
Así mismo la asistencia preventiva y correctiva, es inmediata ante cualquier incidente que lo necesite, ya que el personal CAS y de servicio contratados, cuenta con experiencia en el uso de la marca CISCO, lo cual dinamiza en minimizar los tiempos de respuesta ante los incidentes que ocurren. Se detallan Principales ventajas de la solución de equipamiento CISCO.

7.1. Estandarización de la renovación del Equipamiento de conmutadores de red – SWITCH:

Equipamiento Actual:
La universidad cuenta en su totalidad con switches de la marca CISCO en su CORE y de ACCESO, que actualmente dinamizan la red de una manera eficiente haciendo uso del protocolo propietario EIGRP, el cual permite realizar un balance de carga estable, y realizan actualizaciones de las tablas de rutas solo se

envían cuando se produce un cambio de topología, teniendo la red estable. Sin embargo, la totalidad de los switches de acceso están sin garantía del fabricante.

Se detalla el equipamiento instalado:

MARCA	MODELO	DESCRIPCION DEL EQUIPO	UNIDAD DE MEDIDA	CANTIDAD
CISCO	**C9200L-48P-4X-A**	**SWITCH DE BORDE DE 48 PUERTOS 1000 BASET POE+ Catalyst 9200L 48-port PoE+, 4 x 10G, Network Advantage. Incluye: soportes, licencias y accesorios requeridos**	**unidad**	**36**
CISCO	C9200L-NW-A-48	C9200L Network Advantage, 48-port license	unidad	36
CISCO	C9200L-DNA-A-48-3Y	C9200L Cisco DNA Advantage, 48-port, 3 Year Term license	unidad	36
CISCO	C9200-STACK	Catalyst 9200 Stack Module	unidad	72
CISCO	STACK-T4-50CM	50CM Type 4 Stacking Cable	unidad	36
CISCO	**C9200L-48T-4X-A**	**SWITCH DE BORDE DE 48 PUERTOS 1000 BASET Catalyst 9200 48-port data only, 4 x 10G ,Network Advantage. Incluye: soportes, licencias y accesorios requeridos**	**unidad**	**41**
CISCO	C9200L-NW-A-48	C9200L Network Advantage, 48-port license	unidad	41
CISCO	C9200L-DNA-A-48-3Y	C9200L Cisco DNA Advantage, 48-port, 3 Year Term license	unidad	41
CISCO	C9200-STACK	Catalyst 9200 Stack Module	unidad	82
CISCO	STACK-T4-50CM	50CM Type 4 Stacking Cable	unidad	41
CISCO	**C9200L-24P-4X-A**	**SWITCH DE BORDE DE 24 PUERTOS 1000 BASET POE+ Catalyst 9200L 24-port PoE+, 4 x 10G, Network Advantage. Incluye: soportes, licencias y accesorios requeridos**	**unidad**	**32**
CISCO	C9200L-NW-A-24	C9200L Network Advantage, 24-port license	unidad	32
CISCO	C9200L-DNA-A-24-3Y	C9200L Cisco DNA Advantage, 24-port, 3 Year Term license	unidad	32
CISCO	C9200-STACK	Catalyst 9200 Stack Module	unidad	64
CISCO	STACK-T4-50CM	50CM Type 4 Stacking Cable	unidad	32
CISCO	**C9200L-24T-4X-A**	**SWITCH DE BORDE DE 24 PUERTOS 1000 BASET Catalyst 9200L 24-port data only, 4 x 10G ,Network Advantage. Incluye: soportes, licencias y accesorios requeridos**	**unidad**	**3**
CISCO	C9200L-NW-A-24	C9200L Network Advantage, 24-port license	unidad	3
CISCO	C9200L-DNA-A-24-3Y	C9200L Cisco DNA Advantage, 24-port, 3 Year Term license	unidad	3
CISCO	C9200-STACK	Catalyst 9200 Stack Module	unidad	6
CISCO	STACK-T4-50CM	50CM Type 4 Stacking Cable	unidad	3
CISCO	**C9500-48Y4C-A**	**SWITCH CORE DE CAMPUS DE 48 PUERTOS SFP+ Catalyst 9500 48-port x 1/10/25G + 4-port 40/100G, Advantage. Incluye: soportes, licencias y accesorios requeridos**	**unidad**	**4**
CISCO	C9500-NW-A	C9500 Network Stack, Advantage	unidad	4

CISCO	SFP-H25G-CU3M	25GBASE-CU SFP28 Cable 3 Meter	unidad	8
CISCO	C9500-24Y4C-A	Catalyst 9500 24-port 10/25G and 4-port 40/100G, Advantage	unidad	4
CISCO	PWR-C5-650WAC-R	650W AC 80+ Platinum Config 5 Power Supply front to back cooling	unidad	4
CISCO	C9K-PWR-650WAC-R/2	650W AC Config 4 Power Supply front to back cooling	unidad	4
CISCO	C9K-T1-FANTRAY	Catalyst 9500 Type 4 front to back cooling Fan	unidad	8
CISCO	C9500-DNA-A-3Y	Cisco Catalyst 9500 DNA Advantage 3 Year License	unidad	4
CISCO	QSFP-H40G-CU2M=	40GBASE-CR4 Passive Copper Cable, 2m	unidad	4

Rendimiento:
La marca CISCO, en sus nuevso modelos emergentes para switch borde y core de campus, proporciona una comprensible y completa solución de equipos de Core, Distribución y Acceso, para la conexión de los equipos periféricos de la red LAN. Permitiendo el crecimiento moderno, emergente, rápido y flexible de la red.

Manejabilidad:
Administración centralizada, con la marca Cisco, con soluciones Digital Network Architecture – DNA, puede brindar recopilación de datos de equipos múltiples y obtiene el conocimiento de los dispositivos y aplicaciones, realizar automatizaciones y telemetría, para la toma de decisiones inteligentes autónomas, programadas por el administrador de red, contribuyendo con la ciberseguridad de la red.

Diferenciadores:
La marca CISCO cuenta con los siguientes diferenciadores técnicos respecto a la competencia:

- Equipo diseñado para la necesidad de la red UNP.
- Protocolo EIGRP propietario que mejoran el funcionamiento de la red.
- Gestión centralizada DNA ofrece inteligencia artificial y aprendizaje automático, y facilita detectar y administrar lo que requiere atención.
- Líder por quinto año consecutivo en el cuadrante Gartner, para redes alámbricas e inalámbricas.

Flexibilidad:
La marca Cisco provee a clientes de todos los tamaños de soluciones con los equipos idóneos para integrar a sus equipos, según la necesidad y contexto requerido. El crecimiento de su equipamiento moderno tiene compatibilidad con el equipamiento antiguo, a fin de lograr reutilizar en una misma red distintos modelos.

Gran seguridad:
La marca Cisco ofrece operación con el protocolo 802.1x, 802.1Xrev, MACsec-128, MACsec-256, brindando una seguridad estable en toda la red, así mismo con la gestión DNA se tendrá una visibilidad integral de la red, permitiendo la gestión por perfiles de usuarios y de dispositivos IoT, para un eficiente y eficaz, acceso y segmentación dinámica basados en las necesidades de la UNP.

Prevención de amenazas:
La marca Cisco, con su solución DNA recolecta los datos de la red para detectar donde y cuando ocurrieron vulnerabilidades y/o problemas en la red, pudiendo identificar a nivel de usuario. Usa el aprendizaje automático para resolverlos con rapidez. Esto permite mejorar el rendimiento y la confiabilidad de la red.

7.2. Estandarización de la renovación del Equipamiento de redes inalámbricas ACCESS POINT Y CONTROLADOR INALAMBRICO:

Equipamiento Actual:
La universidad cuenta con un controlador inalámbrico CISCO, que actualmente gestiona a toda la red inalámbrica, y cuenta con Access Point modelos, las cuales están operando dentro del campus, con los protocolos de seguridad y cubriendo las necesidades de los alumnos, administrativos y docentes de la universidad. Sin embargo, no se logra tener una cobertura total a todas las zonas necesarias de la UNP, y el wireless controler y access point sin garantía,

Se detalla el equipamiento instalado:

MARCA	MODELO	DESCRIPCION DEL EQUIPO	UNIDAD DE MEDIDA	CANTIDAD
CISCO	**C9800-40-K9**	**Wireless Controller Cisco Catalyst 9800-40. Incluye: soportes, licencias y accesorios requeridos**	unidad	**1**
CISCO	SC980040K9-173	Cisco Catalyst 9800-40 Wireless Controller	unidad	1
CISCO	C9800-AC-750W-R	Cisco Catalyst 9800-40 750W AC Power Supply, Reverse Air	unidad	1
CISCO	C9800-AC-750W-RED	Cisco Catalyst 9800-40 750W AC Power Supply, Reverse Air	unidad	1
CISCO	**C9115AXI-A**	**ACCESS POINT TIPO INDOOR Cisco Catalyst 9115AX Series. Incluye: soportes, licencias y accesorios requeridos**	unidad	**140**
CISCO	AIR-AP-BRACKET-1	802.11 AP Low Profile Mounting Bracket (Default)	unidad	140
CISCO	DNA-A-3Y-C9115	C9115AX Cisco DNA On-Prem Advantage,3Y Term,Trk Lic	unidad	140
CISCO	AIR-DNA-A-3Y	Wireless Cisco DNA On-Prem Advantage, 3Y Term Lic	unidad	140
CISCO	**AIR-AP1562I-A-K9**	**ACCESS POINT TIPO OUTDOOR CISCO AP 1562i Internal Ant, A Reg Dom. Incluye: soportes, licencias y accesorios requeridos**	unidad	**50**
CISCO	SWAP1560-LOCAL-K9	Cisco 1560 Series Unified Local Mode Software	unidad	50
CISCO	AIR-ACC1530-PMK1	Standard Pole/Wall Mount Kit for AP1530/1560 Series	unidad	50
CISCO	AIR-DNA-A-3Y	Wireless Cisco DNA On-Prem Advantage, 3Y Term Lic	unidad	50

Rendimiento:
La marca CISCO, en sus nuevos Controlador Inalámbricos, provee un alto rendimiento de WLANs y cantidades de Access Point administrados, con fuente redundante, soportando una gran cantidad de clientes en un entorno fácil de administración. Así mismo los emergentes access point, ya soportan WIFI 6 con protocolo 802.11AX, para altas velocidades de conexión de los usuarios.

Manejabilidad:
La marca CISCO, proporciona una administración de equipos segura y centralizada de todos los Access Point. Poder crear grupos de Access Point por tipos de usuarios, diferenciar los accesos y SSIDs, según la necesidad de la UNP.

Diferenciadores:
La marca CISCO cuenta con los siguientes diferenciadores técnicos respecto a la competencia:

- Solución WiFi, que permite administrar diferentes modelos de Access Point, en diferentes versiones de sistemas operativos, lo cual permite una convivencia de equipos antiguos y modernos.
- Controladores que pueden trabajar en Capa 2 y Capa3.
- Los access point emergentes operan con wifi 6, y tienen coexistencias con redes 4G a fin de evitar interferencias de las redes móviles.
- Reconocimiento de aplicaciones en la red, para filtrados de paginas no permitidas por tipo de usuario, incluso por horarios, de manera automática.
- Control, análisis y compatibilidad con Cisco DNA.

Flexibilidad:
Los controladores de la marca CISCO provee a los clientes todos los tamaños de soluciones con la más actualizada protección de seguridad de redes wifi, reduciendo la complejidad y al más bajo costo, así mismo se cuenta con soluciones para brindar cobertura a la totalidad de usuarios de la UNP, y con proyección de crecimiento de un 100% a 5 años futuros.

Gran seguridad:
La marca CISCO, en sus soluciones emergentes de WiFi ofrece protocolos de seguridad para la conexión de los usuarios tal como 802.1x, autenticación por MAC y Portal WEB. Teniendo un control de acceso a la red variable.
Soportada por proteccion de seguridad como: ETA, image signing, secure boot, MACsec encryption, WIPS, WPA2, WPA3, TSL, Encapsulating Security Payload (ESP) Triple DES (3DES) Transform.

Prevención de amenazas:
La marca CISCO, en sus soluciones emergentes de WiFi, proporciona mecanismos de análisis de espectro para la solución inalámbrica, brindando corrección en tiempo real y optimizar la señal para sus usuarios finales, al mismo tiempo al poder estar integrado con la gestión DNA, dinamiza la identificación de amenazas y toma de acciones correctivas inmediatas por parte de la misma arquitectura DNA (previamente habilitada por el administrador de red).

8. Uso que se le dará al equipamiento de red a estandarizar

El uso de la solución de red alámbrica e inalámbrica, tiene el propósito de que el nuevo equipamiento de la marca CISCO que se adquiera, pueda integrarse con eficiencia a los equipos existentes, así mismo, mantener el la compatibilidad y asegurando la protección de la red interna de datos de la UNP, finalmente obtener valor del conocimiento técnico del personal UNP, que al conocer la marca, sus tiempos de respuesta ante incidentes son muy cortos; por este motivo la estandarización de bienes para la renovación/compra de nuevos equipos de red de la marca CISCO responde a esta necesidad.

9. Justificación de la Estandarización

9.1. Que la Entidad posee determinado equipamiento o infraestructura, pudiendo ser maquinarias, equipos, vehículos, u otro tipo de bienes, así como ciertos servicios especializados

La UNP dispone actualmente con la solución de red con equipamiento CISCO en un 97%, el otro 3% están distribuidos en equipos que, a la fecha presentan constantes fallas de otras marcas para una necesidad puntual.
Por lo tanto, la estandarización del equipamiento de red (switch, access point, y wireless controler, para la adquisición de equipos emergentes, se aplicará necesariamente sobre la actual solución instalada, es decir sobre el bien preexistente.

9.2. Que los bienes o servicios que se requiere contratar son accesorios o complementarios al equipamiento o infraestructura preexistente e imprescindibles para garantizar la funcionalidad, operatividad o valor económico de dicho equipamiento o infraestructura.

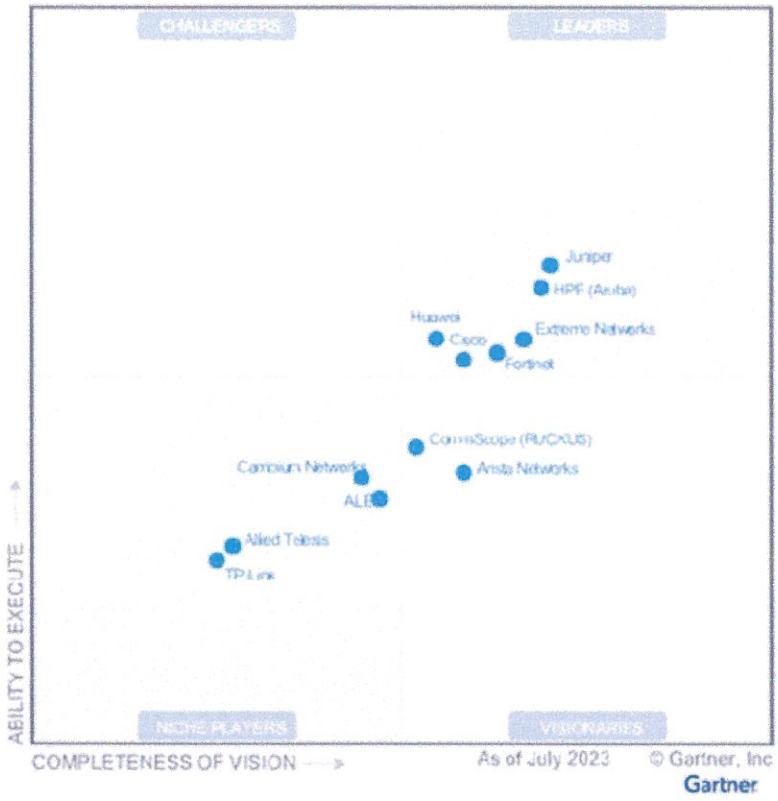
Debido a que actualmente ya se cuenta con la solución de red de equipos SWITCH CORE y BORDE y ACCESS POINT de la marca CISCO, y se tiene configurados para soportar la totalidad de nodos remotos con la marca CISCO, la cual brinda eficiencia con la conectividad de red entre estos, en seguridad y velocidad, trabajando a sus máximas capacidades que el hardware actual permite.
Por ello un cambio de marca en el equipamiento de red ocasionaría problemas en la funcionalidad, operatividad y continuidad de las actividades de la UNP, ya que se tendría que habilitar protocolos estándares que no hacen operar a los equipos en sus máximas capacidades.
Además, se tendría que requerir una nueva capacitación para el equipo técnico especialista de la UNP, teniendo una curva de aprendizaje lento que ocasionaría lentitud en los tiempos de respuesta de los incidentes, y también implicaría incurrir en una inversión de tiempo y dinero no planificado; ya que el equipo técnico UNP están capacitados en el manejo de la solución de red del equipamiento preexistente.
Por lo tanto, la actual inversión efectuada se vería impactada en su implementación.

10. Incidencia económica de la contratación.

La compra de nuevos equipos de la marca CISCO, está dentro del costo promedio de equipos de otras marcas, a continuación, se brinda un cuadro comparativo con la marca ARUBA ya que ambos pertenecen como líderes al cuadro de gartner en redes alámbricas e inalámbricas, estos costos incluyen todos los accesorios requeridos como fuentes redundantes, transceiver, módulos stack, soporte de fábrica, etc, incluido instalaciones a todo costo, según las necesidades de la UNP:

Producto	Precio incluido Impuestos Marca CICO	Precio incluido Impuestos Marca ARUBA
SWITCH CORE 40 SFP+ y 2 QSFP	S/. 157 176.00	S/. 170 340.00
SWITCH TIPO BORDE 48 POE+ (1G) y 4 SFP+	S/. 25 420.00	S/. 27 600.00
SWITCH TIPO BORDE 24 POE+ (1G) y 4 SFP+	S/. 21 200.00	S/. 22 300.00
CONTROLADOR INALAMBRICO	S/. 120 240.00	S/. 135 700.00
ACCESS POINT INDOOR	S/. 5 200.00	S/. 5 520.00
ACCESS POINT OUTDOOR	S/. 6 100.00	S/. 6 820.00

Se debe tener en cuenta que un cambio de marca de la solución de red, generaría una gran inversión de tiempo y dinero debido a que se deberá capacitar e instruir al equipo especialista de la UNP en el uso de la nueva solución, con lo cual el rendimiento de los usuarios se vería afectado. El cambio a otra solución de RED afectaría también a la inversión realizada por los equipos SWITCH CORE vigentes, y los access point vigentes, debido a que requeriría de una inversión no planificada para poder adquirir la nueva solución y migrar las actuales configuraciones.



Fuente: https://www.linkedin.com/posts/kevinrhodescpa_extreme-networks-a-leader-in-2024-gartner-activity-7173029216265957376-nnKq

11. Periodo de vigencia de la estandarización

La estandarización requerida deberá tener una vigencia de tres (03) años, debiendo tener en cuenta que de variar la condiciones que determinaron la estandarización, se pondrá en conocimiento de la Dirección General y el Rectorado de la UNP, a fin de dejar sin efecto la estandarización requerida.

12. Conclusión

Por las razones expuestas y con la finalidad de garantizar la funcionalidad, operatividad, performance y continuidad óptima de las actividades de evaluación y fiscalización ambiental a cargo de la UNP, se recomienda realizar la estandarización con la marca CISCO SYSTEMS, para las compras de equipamiento de red para switches, controlador inalámbricos y access point, por un periodo de tres (03) años.

ANEXO 2

UNIVERSIDAD NACIONAL DE PIURA

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

INFORME TÉCNICO N° 02 PARA LA ESTANDARIZACIÓN DE EQUIPAMIENTO DE LA MARCA HPE PARA LA SOLUCIÓN DE PROCESAMIENTO Y ALMACENAMIENTO DE LA UNP

1. **Nombre de la Oficina**

   Oficina de Tecnología de la Información.

2. **Nombre y Cargo de los responsables de la Evaluación**

   Jassayra Araliz Chulle Chapilliquen
   Jefe de la Oficina de Tecnología de la Información

3. **Fecha**

   Piura, 13 de septiembre de 2024

UNIVERSIDAD NACIONAL DE PIURA
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
RECIBIDO: HORA:
REG. N° 13 SEP 2024 FOLIO N°

4. **Objetivo**

   Establecer la justificación técnica que evidencie la necesidad de estandarizar la adquisición de soluciones de almacenamiento y procesamiento centralizado de misión crítica HPE, la cual albergará los datos de los variados sistemas de información, sistemas administrativos, archivos compartidos y bases de datos, todo ello sobre la infraestructura existente de servidores **HPE Chasis para procesamiento SYNERGY 12000 y HPE Chasis para almacenamiento Storage de la UNP**.

   Esto garantizará la operatividad de todos los servicios informáticos proporcionados por el Centro de Datos de la Oficina de Tecnologías de la Información. Además, asegurará la continuidad en la operatividad, disponibilidad y funcionalidad de todos los servicios informáticos que ofrece el Centro de Datos de la Oficina de Tecnologías de la Información de la Universidad Nacional de Piura.

5. **Marco Legal**

   5.1 El Numeral 29.4 del Artículo 29° del Reglamento de Contrataciones del Estado, establece que: *"... salvo que la Entidad haya implementado el correspondiente proceso de estandarización debidamente autorizado por su Titular, en cuyo caso se agregan las palabras "o equivalente" a continuación de dicha referencia".*

   5.2 En el Anexo N° 1 del Reglamento de Contrataciones del Estado se define Estandarización como *"Proceso de racionalización consistente en ajustar a un determinado tipo o modelo los bienes o servicios a contratar, en atención a los equipamientos existentes."*

   5.3 En tal sentido, y dado que la Directiva N°004-2016-OSCE/CD que refiere los Lineamientos para la Contratación en la que se hace Referencia a Determinada Marca o Tipo Particular de producto, indicando:

"Cuando en una contratación en particular el área usuaria - aquella de la cual proviene el requerimiento de contratar o que, dada su especialidad y funciones, canaliza los requerimientos formulados por otras dependencias - considere que resulta inevitable definir el requerimiento haciendo referencia a fabricación o procedencia, procedimiento de fabricación, marcas, patentes o tipos, origen o producción determinados o descripción que oriente la contratación hacia ellos, deberá elaborar un informe técnico de estandarización debidamente sustentado, el cual contendrá como mínimo:

a. La descripción del equipamiento o infraestructura preexistente de la entidad.
b. La descripción del bien o servicio requerido, indicándose la marca o tipo de producto; así como las especificaciones técnicas o términos de referencia, según corresponda.
c. El uso o aplicación que se le dará al bien o servicio requerido.
d. La justificación de la estandarización, donde se describa objetivamente los aspectos técnicos, la verificación de los presupuestos para la estandarización antes señalados y la incidencia económica de la contratación.
e. Nombre, cargo y firma de la persona responsable de la evaluación que sustenta la estandarización del bien o servicio, y del jefe del área usuaria.
f. La fecha de elaboración del informe técnico."

5.4 Se determina que la única excepción para adquirir bienes o servicios precisando nombre de marca o tipo de producto es la existencia de un proceso de estandarización (Art. 29° del Reglamento de Contrataciones vigente). La Oficina de Tecnologías de la Información de la Universidad Nacional de Piura, define y sustenta en el presente informe, que la ADQUISICIÓN DE UNA SOLUCIÓN DE PROCESAMIENTO Y ALMACENAMIENTO CENTRALIZADO DE MISIÓN CRÍTICA PARA EL CENTRO DE DATOS DE LA OTI deberá ser por un proveedor autorizado por el fabricante respectivo HPE para lo cual se procederá estrictamente con lo descrito he indicado en la Directiva N°004-2016-OSCE/CD y en el punto 5.3 del presente informe.

6. Descripción del Equipamiento o Infraestructura Preexistente

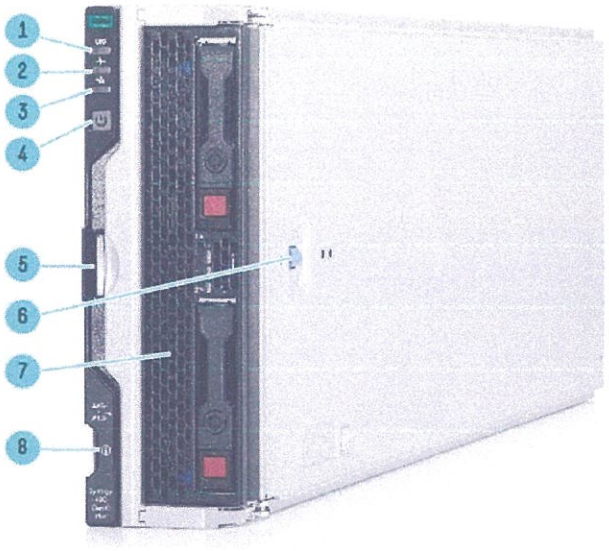
La UNIVERSIDAD NACIONAL DE PIURA, actualmente cuenta con las siguientes soluciones de la marca HPE como componente principal del centro de datos:

- Equipamiento de procesamiento de datos - CHASIS HPE SYNERGY 12000:
    - La solución de procesamiento y almacenamiento centralizado de misión crítica HPE Synergy 12000 está diseñada para albergar los datos de los variados sistemas de información, sistemas administrativos, archivos compartidos y bases de datos de la Universidad Nacional de Piura (UNP). Esta solución garantiza la operatividad, disponibilidad y funcionalidad de todos los servicios informáticos proporcionados por el Centro de Datos de la Oficina de Tecnologías de la Información1.
    - El chasis HPE Synergy 12000 es el componente principal del centro de datos de la UNP y cuenta con las siguientes características2:
    - **Hasta 12 módulos de computación de media altura.**
    - **Diez ventiladores y un módulo de enlace de marco** incluidos con cada sistema.

- **Dos bahías de dispositivos de gestión redundantes.**
- **Inclue seis fuentes de alimentación de eficiencia clase Titanium.**
- **Cuenta con 6 bahías de interconexión para redundancia completa de 3 tejidos.**
- **Dos ranuras para módulos de enlace de marco** que ofrecen enlaces a múltiples marcos a través de una red de gestión privada y aislada.
- **Tecnología de recursos inteligentes HPE** integrada en cada marco y opción para auto-descubrimiento de recursos.

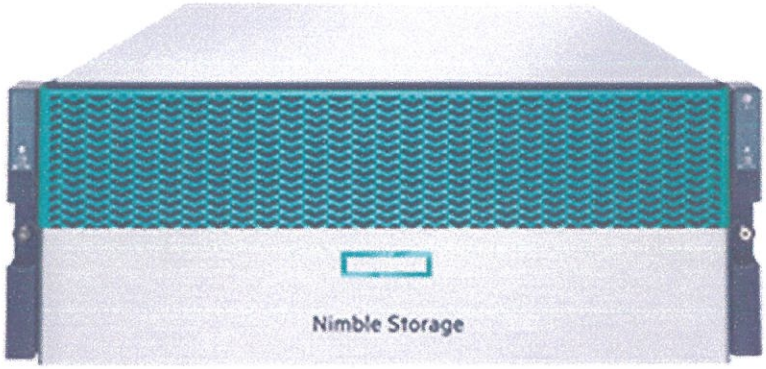
- Equipamiento de procesamiento de datos – Servidor Blade HPE Synergy 480 Gen10 Plus:
  - El **servidor blade HPE Synergy 480 Gen10 Plus** es parte de la infraestructura de procesamiento de datos de la Universidad Nacional de Piura (UNP). Este servidor blade está diseñado para ofrecer un rendimiento y una eficiencia excepcionales, y es compatible con el chasis HPE Synergy 12000.

- El HPE Synergy 480 Gen10 Plus es un módulo de computación que ofrece capacidad, eficiencia y flexibilidad superiores en un factor de forma de media altura y dos sockets. Está diseñado para soportar cargas de trabajo exigentes y es alimentado por los últimos procesadores Intel® Xeon® Scalable. Este módulo también soporta hasta 3TB de memoria HPE DDR4 SmartMemory, opciones flexibles de controladores de almacenamiento y tres conectores de E/S.

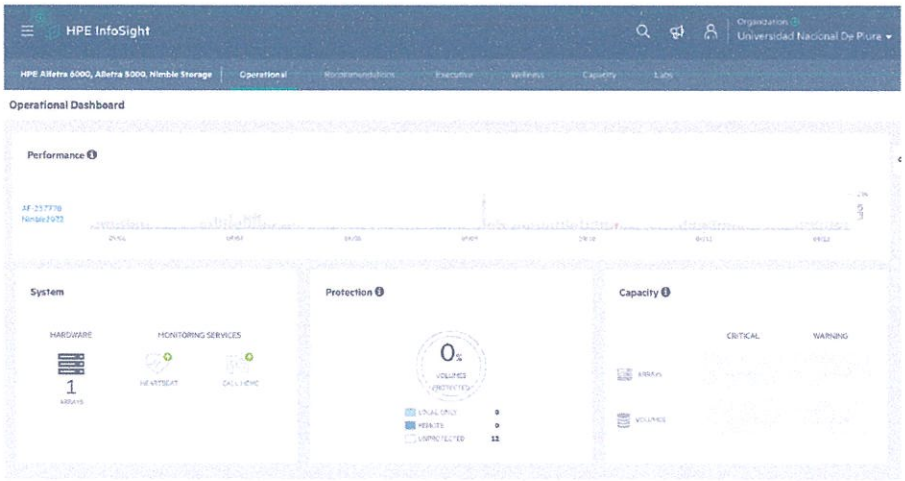


- Equipamiento de almacenamiento de datos – Storage Blade HPE Nimble HF20

  - El HPE Nimble Storage HF20 es un array de almacenamiento flash híbrido diseñado para cargas de trabajo mixtas, tanto primarias como secundarias. Algunas de sus características incluyen4:
    - Controlador dual adaptable con puertos 10GBASE-T de 2 puertos.
    - Reducción de datos mediante deduplicación y compresión de bloques variables en línea.
    - Arquitectura flash mejorada combinada con análisis predictivo HPE InfoSight para un acceso rápido y confiable a los datos con una disponibilidad garantizada del 99.9999%.
    - Simplicidad radical en la implementación y gestión, con movilidad de datos a la nube a través de HPE Cloud Volumes.
    - Rendimiento flash para cargas de trabajo mixtas con respuesta en sub-milisegundos y mayor eficiencia que otros arrays híbridos.



- Solución de monitoreo online – HPE Infosight
    - HPE InfoSight es una solución de monitoreo en línea que proporciona análisis predictivo mejorado. Algunas de sus características incluyen la capacidad de predecir con precisión las necesidades de capacidad, rendimiento y ancho de banda, y realizar actualizaciones específicas. HPE InfoSight está diseñado para hacer que la infraestructura sea autónoma, recolectando datos y aprendiendo de las cargas de trabajo de los clientes para hacer que todos los clientes sean más inteligentes. La plataforma está pavimentando el camino hacia una infraestructura autónoma que se autogestiona, se auto-repara y se auto-optimiza



7. Descripción del Bien a Estandarizar

El presente documento tiene por finalidad, establecer el sustento para la estandarización la ampliación del equipamiento de procesamiento y almacenamiento, de la marca HEWLETT PACKARD ENTERPRISE (HPE).

La adquisición del equipamiento con la marca HPE es imprescindible para garantizar la operatividad eficiente de la solución de la red de datos de la universidad, ya que actualmente los servidores operan dentro del chasis HPE con comunicación cifrada y propietaria de la marca, la cual ha demostrado una eficiente operación.
Así mismo la asistencia preventiva y correctiva, es inmediata ante cualquier incidente que lo necesite, ya que el personal CAS y de servicio contratados, cuenta con experiencia en el uso de la marca HPE, lo cual dinamiza en minimizar los tiempos de respuesta ante los incidentes que ocurren. Se detallan Principales ventajas de la solución de equipamiento HPE.

7.1. Estandarización de las ampliaciones del Equipamiento de Servidores de Procesamiento (para procesamiento de aplicaciones).

Equipamiento para estandarizar:

- Chasis de Procesamiento HPE Synergy 12000.
- Servidores tipo blade HPE Synergy 480 Gen11 Plus

Rendimiento:
La marca HPE, en sus nuevos modelos emergentes proporciona una comprensible y completa solución moderno, emergente, rápido y flexible de la red.

Manejabilidad:
Administración centralizada, con la marca HPE, puede brindar recopilación de datos de equipos múltiples y obtiene el conocimiento de los dispositivos y aplicaciones, realizar automatizaciones y telemetría, para la toma de decisiones inteligentes autónomas, programadas por el administrador de red, contribuyendo con la ciberseguridad de la red.

Diferenciadores:
La marca HPE cuenta con InfoSight es una solución de monitoreo en línea que proporciona análisis predictivo mejorado. Algunas de sus características incluyen la capacidad de predecir con precisión las necesidades de capacidad, rendimiento y ancho de banda, y realizar actualizaciones específicas. HPE InfoSight está diseñado para hacer que la infraestructura sea autónoma, recolectando datos y aprendiendo de las cargas de trabajo de los clientes para hacer que todos los clientes sean más inteligentes. La plataforma está pavimentando el camino hacia una infraestructura autónoma que se autogestiona, se auto-repara y se auto-optimiza.

Flexibilidad:
La marca HPE provee a clientes de todos los tamaños de soluciones con los equipos idóneos para integrar a sus equipos, según la necesidad y contexto requerido. El crecimiento de su equipamiento moderno tiene compatibilidad con el equipamiento antiguo.

Gran seguridad:
La marca HPE ofrece operación de datos encriptados y eficiente y eficaz, acceso y segmentación dinámica basados en las necesidades de la UNP.

Prevención de fallas:
La marca HPE, cuenta con soporte directo de la marca, y de manera proactiva su soporte monitorea las vulnerabilidades que pudiesen suscitarse.

7.2. Estandarización de la ampliación del Equipamiento de almacenamiento storage:

Equipamiento para estandarizar:

- Chasis de almacenamiento centralizado de misión crítica con capacidad efectiva de 400 TB como minimo.

- **Rendimiento:**
  La marca HPE, en sus nuevos modelos emergentes proporciona una comprensible y completa solución moderno, emergente, rápido y flexible de la red, con sistema de almacenamiento ofrecido deberá ser un arreglo All Flash NVMe de misión crítica con 99.9999% de disponibilidad o superior garantizado con información pública en el sitio web del fabricante claramente para el modelo ofrecido.

  - El sistema de almacenamiento ofrecido deberá soportar la activación de Calidad de Servicio para asegurar un tiempo de respuesta adecuado para las aplicaciones críticas. Deberá permitir definir diferentes tiempos de servicio/respuesta para diferentes unidades lógicas de aplicación.
  - La funcionalidad de Calidad de Servicio deberá permitir definir el límite mínimo y máximo de IOPS y/o Ancho de Banda requerido para una unidad lógica determinada asociada a una aplicación que se ejecuta en sistema.
  - Será posible cambiar en tiempo real con Calidad de Servicio, IOPS y Ancho de Banda.
  - El sistema de almacenamiento deberá permitir la creación de Snapshots basados en controlador (al menos 1000 copias para un volumen determinado).
  - El sistema de almacenamiento ofrecido deberá admitir más de 10,000 volúmenes base sin incluir snapshots ni clones.
  - El sistema de almacenamiento ofrecido deberá soportar la actualización en línea del firmware sin disrupción del servicio.
  - El arreglo de almacenamiento debe admitir la replicación de datos basada en hardware a nivel de controlador con todos los modelos de la familia ofrecida del sistema de almacenamiento.
  - El arreglo de almacenamiento ofrecido debe tener la capacidad de proporcionar una replicación activa/activa con opción de Clúster extendido a distancias metropolitanas para lograr RPO y RTO de Cero. En esta configuración se puede tener acceso simultáneo de lectura y escritura a los volúmenes replicados entre los datacenters Primario y Secundario.
  - La replicación activa / activa debe ser compatible con todos los sistemas operativos conocidos como VMware, Redhat, Windows, etc.
  - El sistema de almacenamiento ofrecido deberá tener la capacidad de replicar volúmenes agrupados por aplicación o servicios, de forma que se asegure la consistencia de las aplicaciones replicadas

- **Manejabilidad:**
  Administración centralizada, con la marca HPE, puede brindar recopilación de datos de equipos múltiples y obtiene el conocimiento de los dispositivos y aplicaciones, realizar automatizaciones y telemetría, para la toma de decisiones inteligentes autónomas, programadas por el administrador de red, contribuyendo con la ciberseguridad de la red.

- El sistema de almacenamiento deberá admitir plataformas de sistemas operativos y clústeres líderes en la industria, incluidos Windows Server, VMware ESXI, Red Hat Enterprise Linux, SUSE Enterprise Server (SLES), Oracle Linux, Ubuntu, HP-UX, IBM AIX, Solaris, etc.
- El sistema de almacenamiento ofrecido deberá contar con al menos dos controladores All-NVMe.

- **Diferenciadores:**
  La marca HPE cuenta con la opción de unificar sus distintas plataformas de almacenamiento:
  - El sistema de almacenamiento ofrecido deberá soportar la falla simultanea de al menos 2 discos, sin que ocurra una pérdida de datos o afectación del servicio.
  - sistema de almacenamiento ofrecido deberá reservar un espacio de Spare global distribuido, que permita reconstruir los datos en caso de falla de cualquier disco del sistema. El espacio de Spare global se configurará según las mejores prácticas del fabricante, y deberá ser adicional a la capacidad requerida.
  - El sistema de almacenamiento deberá incluir el licenciamiento necesario para encriptación de los datos a nivel de discos, sin necesidad de ningún software de encriptación. El sistema de almacenamiento debe permitir su integración con un manejador de llaves externo KMIP.
  - El sistema de almacenamiento ofrecido deberá configurarse sin puntos únicos de falla a nivel de controladoras, memoria caché, ventilador, fuente de alimentación, etc.
  - El sistema de almacenamiento ofrecido deberá tener al menos 256 GB de memoria entre ambos controladores.
  - El sistema de almacenamiento ofrecido deberá tener CPU x86 con al menos 32 cores o núcleos entre ambos controladores.
  - El sistema de almacenamiento ofrecido deberá estar certificado para soportar conexiones por Fiber Channel (FCP) e iSCSI.
  - El sistema de almacenamiento ofrecido debe incluir el licenciamiento necesario para replicar hasta toda su capacidad instalada a través de conexiones FC o Ethernet, hacia otro sistema del mismo modelo.
  - El sistema de almacenamiento ofrecido debe incluir virtualización nativa para que cualquier volumen lógico o Lun distribuya su capacidad y carga de IO entre todos los discos instalados. No se aceptarán sistemas que dedican discos físicos separados para cada aplicación, lo cual restringe su desempeño.
  - El sistema de almacenamiento ofrecido deberá incluir funcionalidades para reducir el consumo de espacio en disco como Thin Provisioning, Deduplicación y Compresión. Estas funcionalidades deberán tener la flexibilidad de poder habilitarse o deshabilitarse por cada volumen al momento de durante su creación.
  - El sistema de almacenamiento ofrecido deberá tener disponibles para su uso las funcionalidades de Thin Provisioning, Snapshot, Replicación remota, Deduplicación, Compresión, Monitoreo de Performance y Calidad de Servicio (QoS) desde el primer día y para toda la capacidad instalada del sistema.

- **Flexibilidad:**
  La marca HPE provee a clientes de todos los tamaños de soluciones con los equipos idóneos para integrar a sus equipos, según la necesidad y contexto requerido. El crecimiento de su equipamiento moderno tiene compatibilidad con el equipamiento antiguo.
  - Administración de múltiples sistemas de almacenamiento a través de una única consola de datos nativa de nube.

- Panel Principal con información del número total de sistemas, volúmenes, hosts, capacidad e información de rendimiento de los principales sistemas y volúmenes.
- Control de acceso común basado en roles (RBAC) para administrar múltiples sistemas a través de una única consola de datos, en lugar de crear usuarios y asignar roles individualmente en cada arreglo de discos.
- La consola deberá recomendar el sistema más adecuado (si hubiera más de uno) para cada aplicación, en función de la carga de trabajo y basado en el etiquetado de los volúmenes por aplicación.
- Deberá ser capaz de recomendar actualizaciones de software aplicables a la configuración específica del sistema de almacenamiento, previniendo afectaciones del servicio por aplicar actualizaciones no validadas o incompatibles.
- Admitirá el aprovisionamiento estático y dinámico
- Deberá ser capaz de expandir, redimensionar los volúmenes persistentes dados a las aplicaciones state fulset.
- Podrá crear y eliminar snapshots.
- Soportará el volumen de bloques CSI Raw, así como la clonación de volúmenes CSI.
- Soporte tanto para Fiber Channel como para iSCSI.

- **Gran seguridad:**
  La marca HPE ofrece operación de datos encriptados y eficiente y eficaz, acceso y segmentación dinámica basados en las necesidades de la UNP.

- **Prevención de fallas:**
  La marca HPE, cuenta con soporte directo de la marca, y de manera proactiva su soporte monitorea las vulnerabilidades que pudiesen suscitarse.
  - Proporcionar la ruta o saltos de versión requeridos para actualizar a la versión recomendada, información de versión previa de firmware, opción de comprobación del sistema antes de aplicar una actualización, y nivel de severidad para aplicar la actualización recomendada.
  - El panel de control resaltará claramente si hay algún problema con el sistema, y proporcionará información detallada sobre el problema.
  - Proporcionar un monitoreo de rendimiento granular del sistema casi en tiempo real, con intervalos de al menos 5 minutos. Permitirá crear informes personalizados en formato CSV y PDF sin necesidad de aplicar ninguna configuración ni instalar un dispositivo o software adicionales.
  - Proporcionar información del nivel de utilización general del sistema, analizando varios parámetros como IOPS, Throughput en MB/seg, tamaño de bloque de IO, etc.
  - Proporcionar información de utilización del espacio consumido en porcentaje por aplicación etiquetada en el sistema de almacenamiento.
  - Proporcionar el estado de al menos los 5 volúmenes principales con mayor latencia.

8. Uso que se le dará al equipamiento de red a estandarizar

El uso de la solución de red alámbrica e inalámbrica, tiene el propósito de que el nuevo equipamiento de la marca HPE que se adquiera, pueda integrarse con eficiencia a los equipos existentes, así mismo, mantener el la compatibilidad y asegurando la protección de la red interna de datos de la UNP, finalmente obtener valor del conocimiento técnico del personal UNP, que al conocer la marca, sus tiempos de respuesta ante incidentes son muy cortos; por este motivo la estandarización de bienes para la renovación/compra de nuevos equipos de red de la marca HPE responde a esta necesidad.

La adquisición de la solución de almacenamiento centralizado de misión crítica marca HPE o equivalente permitirá incrementar la capacidad actual de almacenamiento centralizado, con la finalidad de proyectar el crecimiento de los archivos digitales de las diversas aplicaciones web o sistemas de información, además de proyectar el crecimiento de las bases de datos tanto de información transaccional como de la información de la planilla electrónica cuyo crecimiento es voluminoso, asimismo esta solución de almacenamiento permitirá generara nuevos proyectos de tecnologías de la información basados en tecnologías disruptivas tales como machine learning, big data entre otros.

Además, al contar con la plataforma de servidores de computadoras de alta gama de misión crítica en marca HPE SYNERGY 12000, esta permitirá integrarse de forma nativa, con el objetivo de contar con las diversas funcionalidades que permitirán tener el mejor desempeño en su funcionamiento.

9. Justificación de la Estandarización

En cumplimiento de la Directiva N 004-2016-OSCE/CD, "Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular", se ha evaluado las razones técnicas para la Adquisición de una Solución de Almacenamiento Centralizado de Misión Crítica de la Marca HPE o Equivalente para la Oficina de Tecnologías de la Información y Comunicaciones", lo que cual se detalla a continuación.

9.1. Que la Entidad posee determinado equipamiento o infraestructura, pudiendo ser maquinarias, equipos, vehículos, u otro tipo de bienes, así como ciertos servicios especializados

La UNP dispone actualmente con la solución de red con equipamiento HPE en un 60%, el otro 40% están distribuidos en equipos HPE descontinuados que a la fecha presentan constantes fallas y no tienen soporte de la marca.

Por lo tanto, la estandarización del equipamiento para la adquisición de equipos emergentes de procesamiento y almacenamiento se aplicará necesariamente sobre la actual solución instalada, es decir sobre el bien preexistente.

9.2. Que los bienes o servicios que se requiere contratar son accesorios o complementarios al equipamiento o infraestructura preexistente e imprescindibles para garantizar la funcionalidad, operatividad o valor económico de dicho equipamiento o infraestructura.

Debido a que actualmente ya se cuenta con la solución de servidores procesamiento y almacenamiento de la marca HPE, y se tiene configurados para soportar el 60% de las aplicaciones y almacenamiento de la información, con la marca HPE, la cual brinda eficiencia con la operación de las aplicaciones y base de datos, en seguridad y velocidad, trabajando a sus máximas capacidades que el hardware actual permite.

Por ello un cambio de marca en el equipamiento de red ocasionaría problemas en la funcionalidad, operatividad y continuidad de las actividades de la UNP, ya que se tendría que habilitar protocolos estándares que no hacen operar a los equipos en sus máximas capacidades.

Además, se tendría que requerir una nueva capacitación para el equipo técnico especialista de la UNP, teniendo una curva de aprendizaje lento que ocasionaría lentitud en los tiempos de respuesta de los

incidentes, y también implicaría incurrir en una inversión de tiempo y dinero no planificado; ya que el equipo técnico UNP están capacitados en el manejo de la solución de red del equipamiento preexistente. Por lo tanto, la actual inversión efectuada se vería impactada en su implementación.

10. Incidencia económica de la contratación.

La compra de nuevos equipos de la marca HPE, está dentro del costo promedio de equipos de otras marcas, a continuación, se brinda un cuadro comparativo con la marca DELL ya que ambos pertenecen como líderes al cuadro de gartner en redes alámbricas e inalámbricas, estos costos incluyen todos los accesorios requeridos como fuentes redundantes, transceiver, módulos stack, soporte de fábrica, etc, incluido instalaciones a todo costo, según las necesidades de la UNP:

Producto	Precio incluido Impuestos Marca HPE	Precio incluido Impuestos Marca DELL
Chasis para servidores	Existente en la entidad	S/ 120,000.00
Servidores Blade	Existente en la entidad	S/ 160,000.00
Servidores Almacenamiento	Existente en la entidad	S/ 1,000,000.00

Con la finalidad de proteger la inversión efectuada en la adquisición e implementación del equipamiento, es necesario la Adquisición de una Solución de Procesamiento y Almacenamiento Centralizado de misión crítica, los cuales son accesorios complementarios al equipamiento y software adquirido, esto con la finalidad de garantizar el continuidad y funcionalidad de la plataforma de Servidores de Computadoras de Alta Gama de misión crítica de la infraestructura tecnológica del Centro de Datos de la UNP.

De no contar con la adquisición de una solución de almacenamiento centralizado de misión crítica marca HPE o equivalente, generará el riesgo de interrumpir todos los servicios informáticos tales como autenticación de usuarios, archivos compartidos, base de datos y en consecuencia no se dispondrá de ningún servicio informático, ya que toda la infraestructura de servidores virtualizados se montan sobre el almacenamiento centralizado y ésta al llegar a su capacidad total podría corromper los datos generando la perdida de la información en general. afectando a los servicios informáticos que se brinda a las distintas instituciones públicas y privadas. Además, de adquirir una solución de almacenamiento de distinta marca podría generar costos adicionales en equipos adicionales para su integración con los servidores de computadoras de misión crítica HPE SYNERGY 12000, además de volver a capacitar al personal y generando un punto de falla a toda la infraestructura tecnológica del Centro de Daos de la UNP.

La adquisición de una solución de almacenamiento centralizado de misión crítica marca HPE, son bienes complementarios a la plataforma de servidores de computadoras de alta gama de misión crítica marca HPE SYNERGY12000.

Se debe mencionar que una estandarización incidirá favorablemente en la parte económica; sin embargo, de realizar la adquisición en otra marca, pondría en riesgo el adecuado funcionamiento de la plataforma de servidores de computadoras de alta gama de misión crítica HPE SYNERGY12000, dado que no contaríamos con los componentes originales y el personal especializado para el soporte técnico ante inconveniente en el funcionamiento, conllevando un riesgo en términos de tiempo y costos para la entidad, perjudicando la atención de los requerimientos de todos los servicios informáticos que brinda del Centro de Datos de la UNP.

11. Periodo de vigencia de la estandarización

La estandarización requerida deberá tener una vigencia de tres (03) años, debiendo tener en cuenta que de variar la condiciones que determinaron la estandarización, se pondrá en conocimiento de la Dirección General y el Rectorado de la UNP, a fin de dejar sin efecto la estandarización requerida.

12. Conclusión

Por las razones expuestas y con la finalidad de garantizar la funcionalidad, operatividad, performance y continuidad óptima de las actividades de evaluación y fiscalización ambiental a cargo de la UNP, se recomienda realizar la estandarización con la marca HEWLETT PACKARD ENTERPRISE, para las compras de equipamiento relacionado a soluciones de procesamiento y almacenamiento de datos, por un periodo de tres (03) años.

ANEXO 3

UNIVERSIDAD NACIONAL DE PIURA

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

INFORME TÉCNICO N° 03 PARA LA ESTANDARIZACIÓN PARA ADQUISICIÓN DE UNA SOLUCIÓN DE CIBERSEGURIDAD CENTRALIZADO EN LA MARCA CHECKPOINT PARA LA PROTECCION EN LA RED EXTERNA E INTERNA DE LA UNIVERSIDAD NACIONAL DE PIURA (UNP)

I. NOMBRE DEL ÁREA

Oficina de Tecnologías de la Información (OTI)

II. NOMBRE Y CARGO DE LOS RESPONSABLES DE LA EVALUACIÓN

Jassayra Araliz Chulle Chapilliquen
Jefe de la Oficina de Tecnología de la Información

UNIVERSIDAD NACIONAL DE PIURA
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
RECIBIDO: 05 SEP 2024 HORA:
REG N° FOLIO N°

III. FECHA

Piura, 05 de septiembre del año 2024

IV. PROPÓSITO

El presente informe tiene por finalidad, justificar la necesidad de implementar una solución unificada basada en la marca Checkpoint, protegiendo la infraestructura de red interna y externa de la Universidad. Estandarizando esta marca, garantizamos el cumplimiento de los estándares de seguridad más exigentes, reduciendo el riesgo de sufrir ataques cibernéticos. Checkpoint ofrece una amplia gama de funcionabilidades únicas de seguridad que protegerán los datos más sensibles de la Universidad.

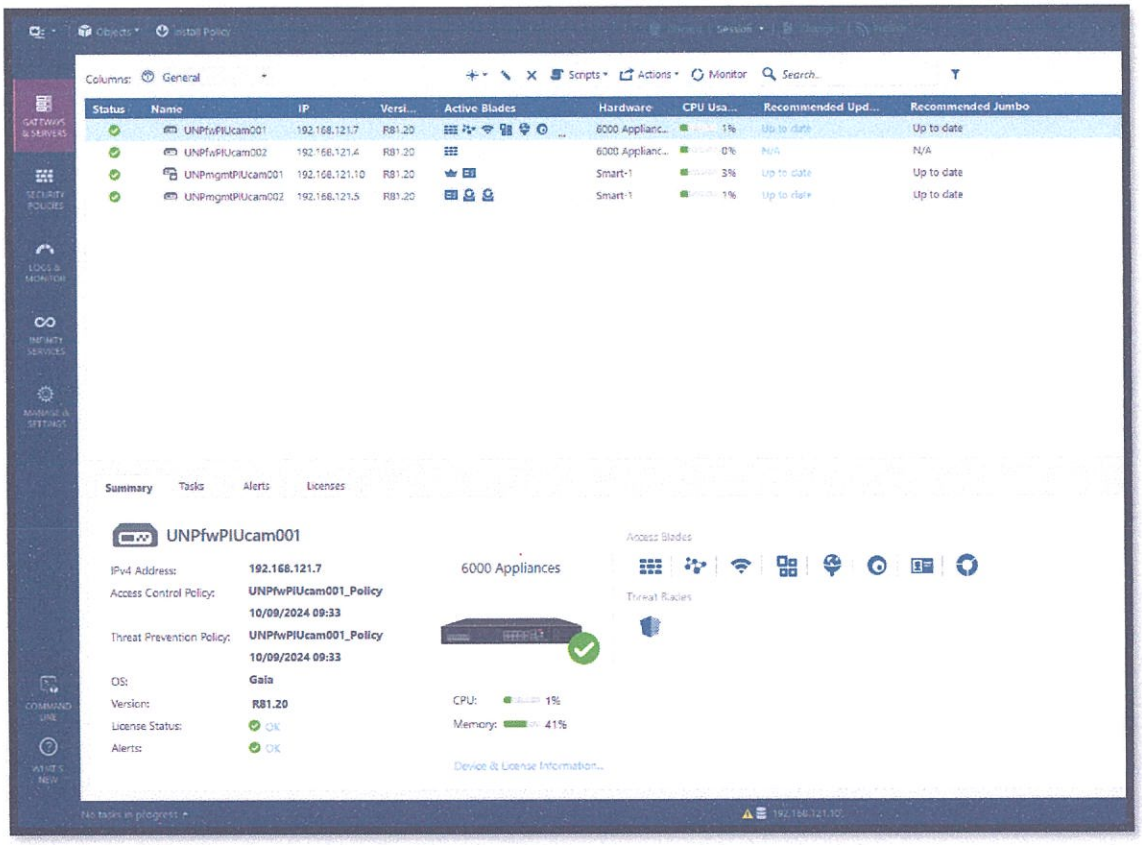
El equipamiento de red actual de la UNP, demostrando cada vez ser confiable, es fundamental tener la continuidad de la solución ya que presenta actualizaciones que contribuyen con la prevención de las nuevas amenazas, mitigando el riesgo elevado de fallas y vulnerabilidades, comprometiendo la seguridad de la red.
Es imperativo renovar este equipamiento con soluciones de última generación, como las ofrecidas por Checkpoint, para garantizar la continuidad de las operaciones y la protección de los datos.

V. DESCRIPCION DEL EQUIPAMIENTO O INFRAESTRUCTURA PREEXISTENTE

La Universidad Nacional de Piura, actualmente cuenta con el equipo principal de ciberseguridad que es el corazón de la protección de toda la institución con un equipo NGTX modelo 6900, actualmente con el firmware recomendado siendo este el 3.10.0-1160.15.2cpx86_64 en la versión del R81.20, instalado en el Data center de la entidad, teniendo como función principal proteger a todos los servidores que alojan la base de datos y aplicaciones de la Universidad.

El firewall Checkpoint 6900 desempeña un papel crucial en la prevención de ataques de virus, troyanos, ransomware y malware, bloqueando las amenazas antes de que puedan comprometer nuestros sistemas. Además, su potente motor de detección protege contra spyware, adware y

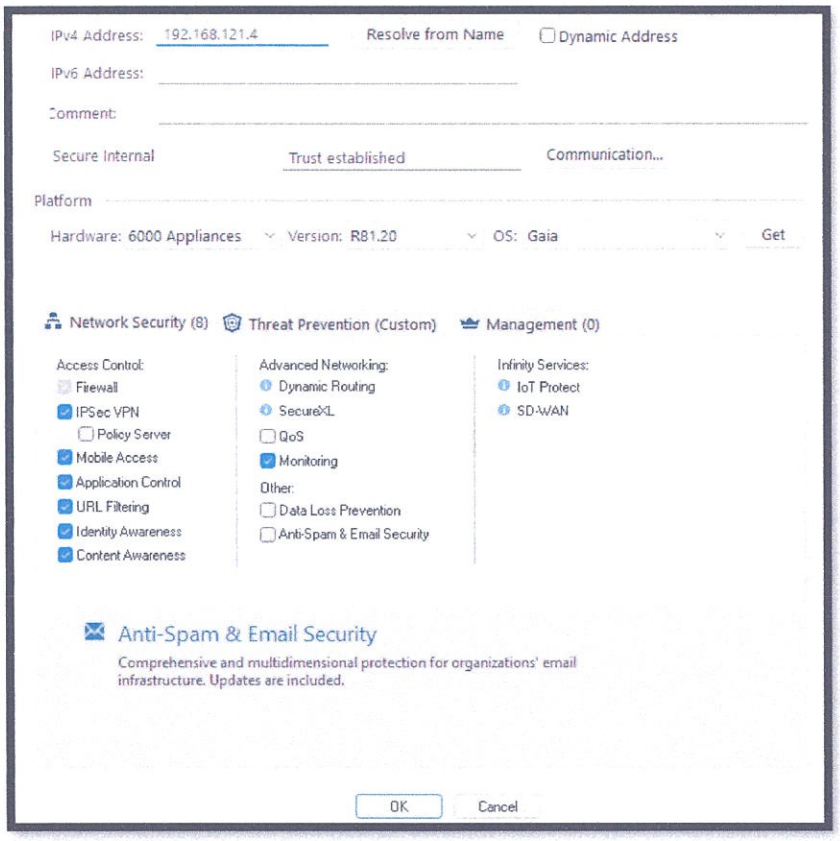
phishing, evitando que información confidencial sea robada o que se instalen programas maliciosos en nuestros equipos.



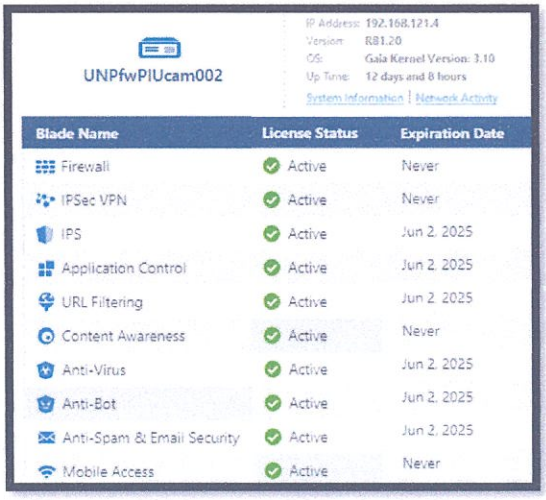
Smartconsole R81.20 – interfaz topológica

Gracias a la versión del Software R81.20 "v9700" perteneciente al año 2024 podemos tener una consola de administración unificada en donde agregamos nuestros equipos de seguridad tal como mostramos en la imagen previa, dado por un gestor en la administración.

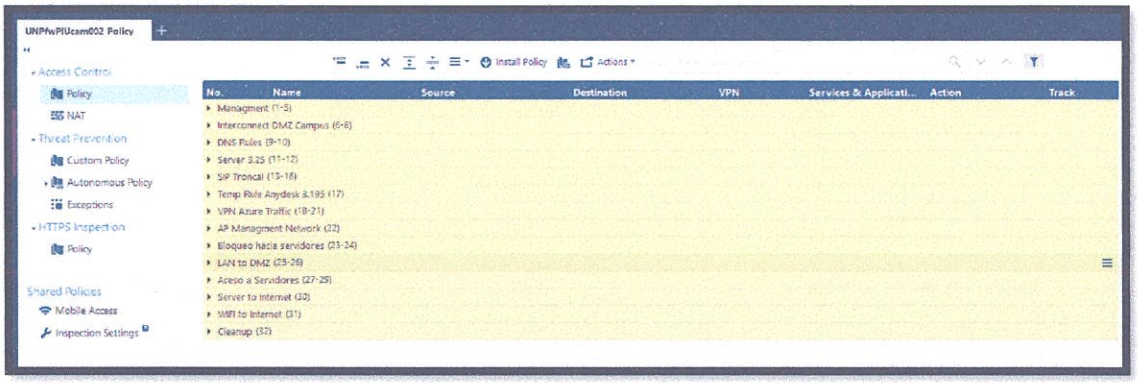
Gracias a la adquisición del equipamiento de seguridad del firewall 6900 tenemos los Blades activos para dicho appliance , este equipo de gestión para la protección de la base de datos y servidores manejándolo por una IP de gestión 192.168.121.4 tal como nos muestra en la siguiente imagen.



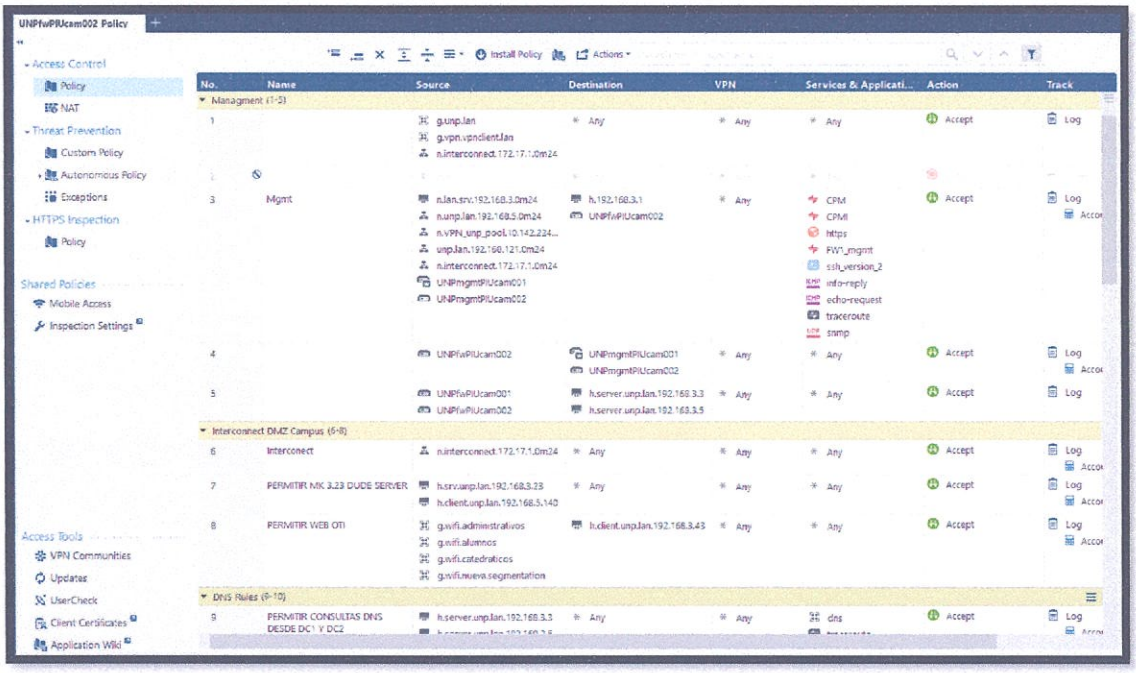
Muestra de los Blades configurados-chek azul



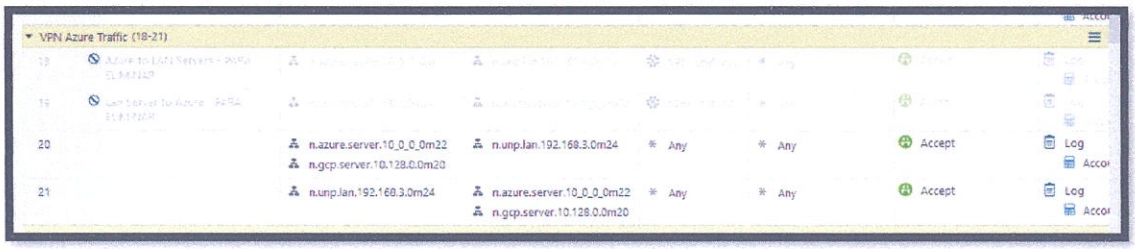
Blades- License Status – Expiration June 2025



Grupo de politicas de seguridad para el firewall 6900



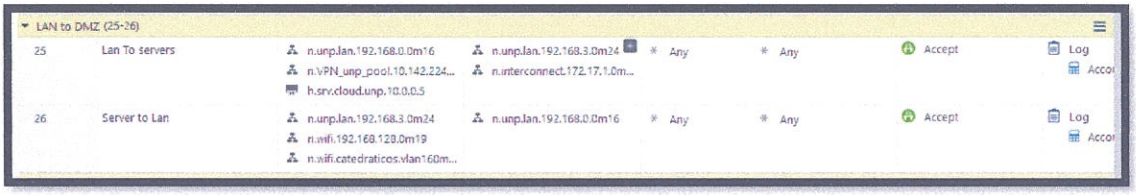
Despliegue de las políticas de seguridad, vista de los servicios y aplicaciones.



Vista de VPN Azure tráfico.

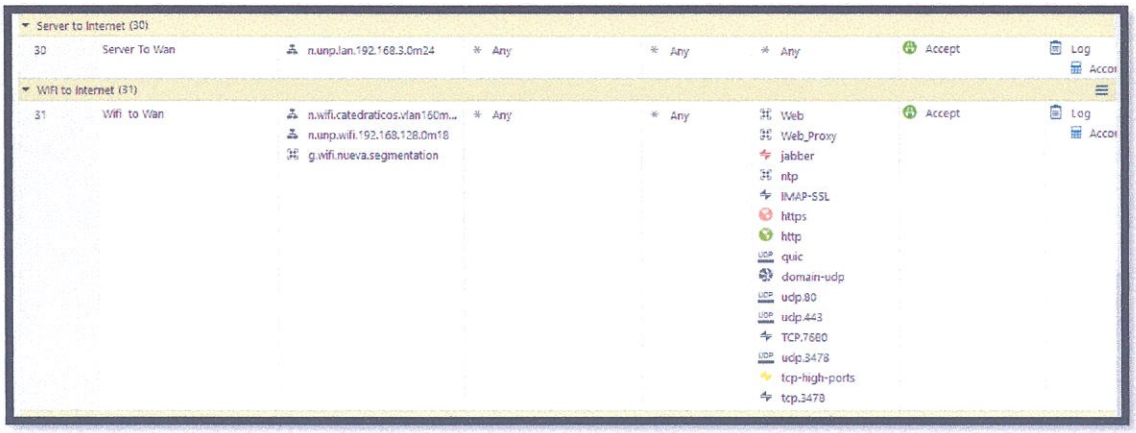
Bloqueo acceso desde wifi de la vlan alumnos hacia los servidores.

En la imagen anterior podemos observar la política configurada para restringir el acceso a todos los que se conectan por wifi hacia los servidores protegiendo la base de datos y aplicaciones de la Entidad.



Grupo de políticas de la LAN hacia la DMZ

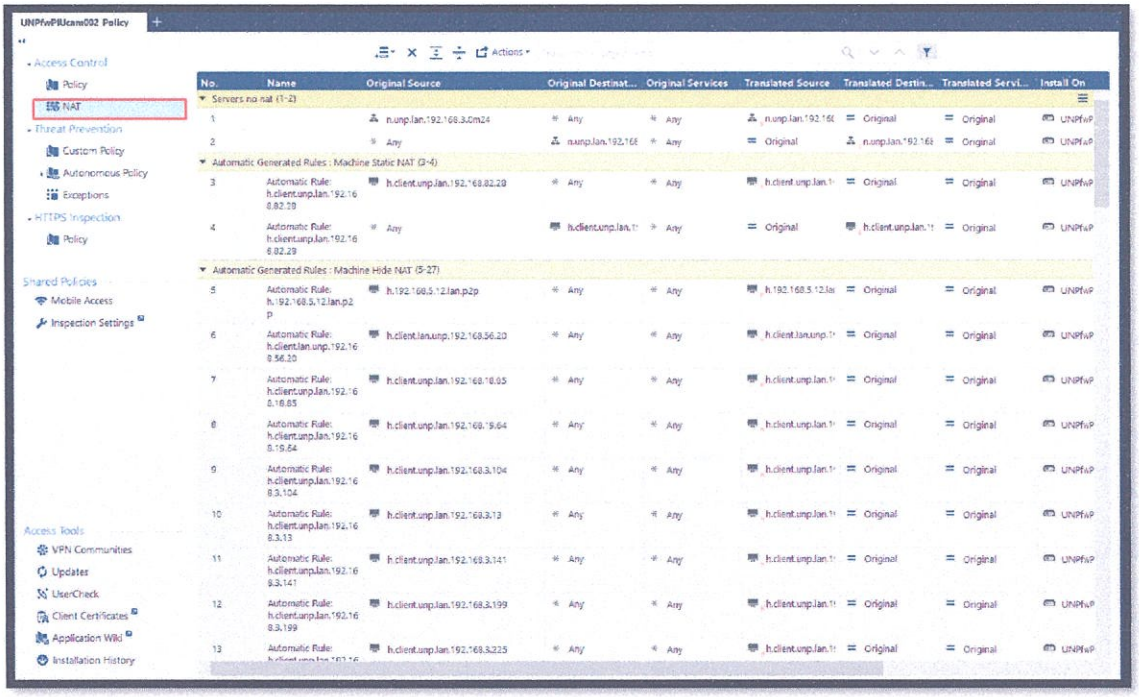
Grupo de políticas para el acceso a los Servers



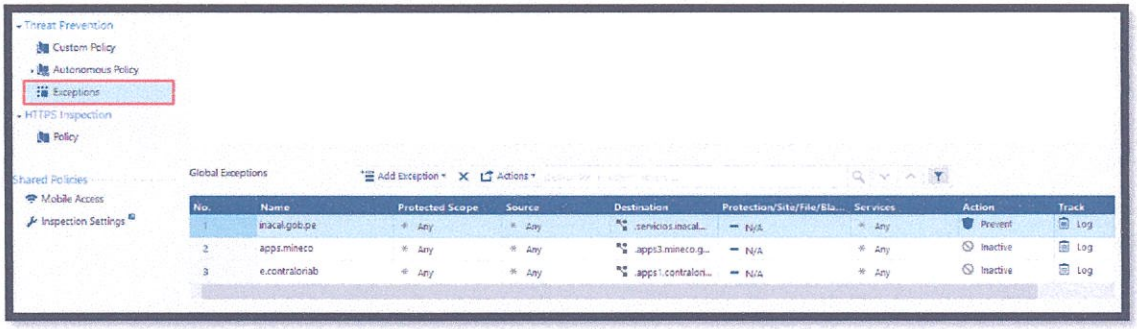
Políticas para Wifi hacia la WAN creación por aplicaciones y servicios

UNIVERSIDAD NACIONAL DE PIURA

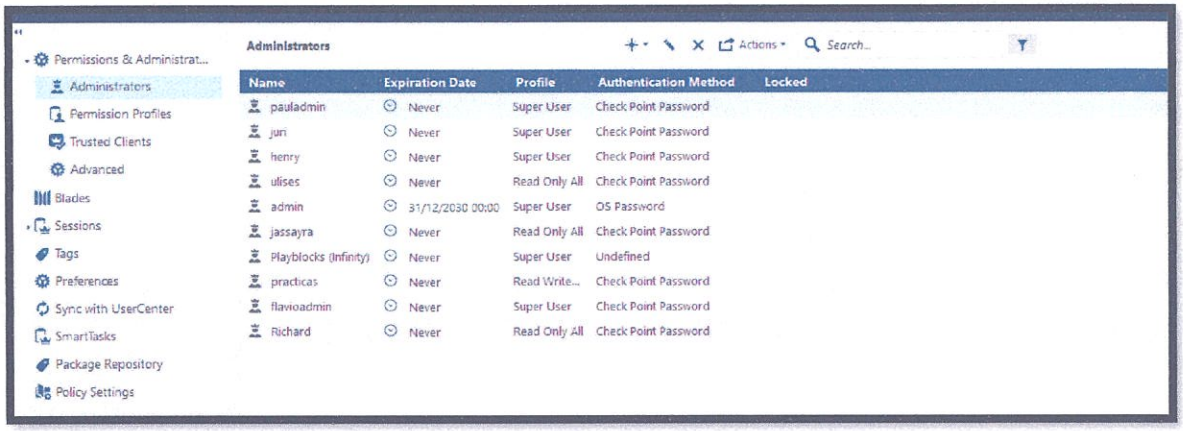
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN



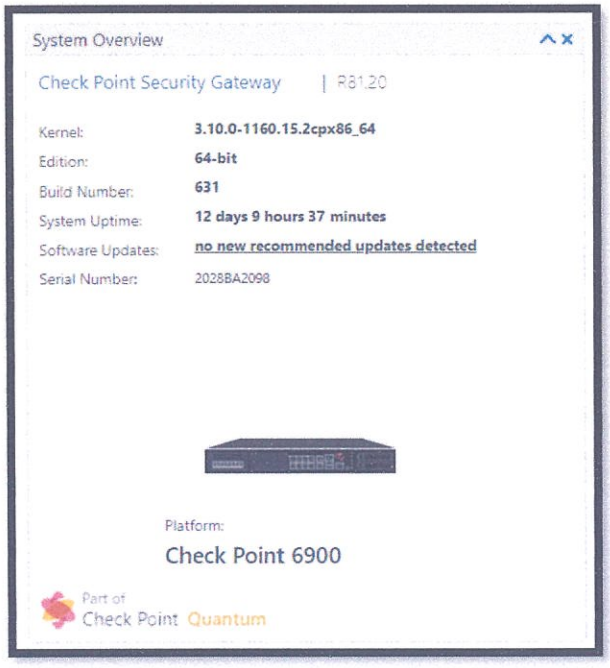
Grupo de NAT, descripción de Server y reglas automáticas



Interfaz de las excepciones configuradas para el FW-6900



Podemos ver los administradores de los equipos Checkpoint

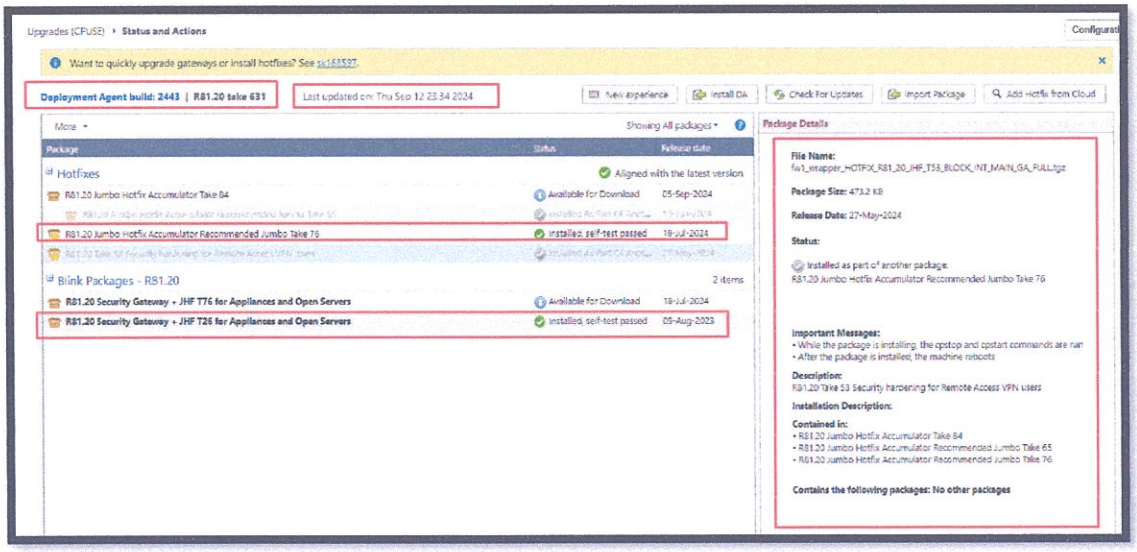


Overview del equipo S/N :2028BA2098

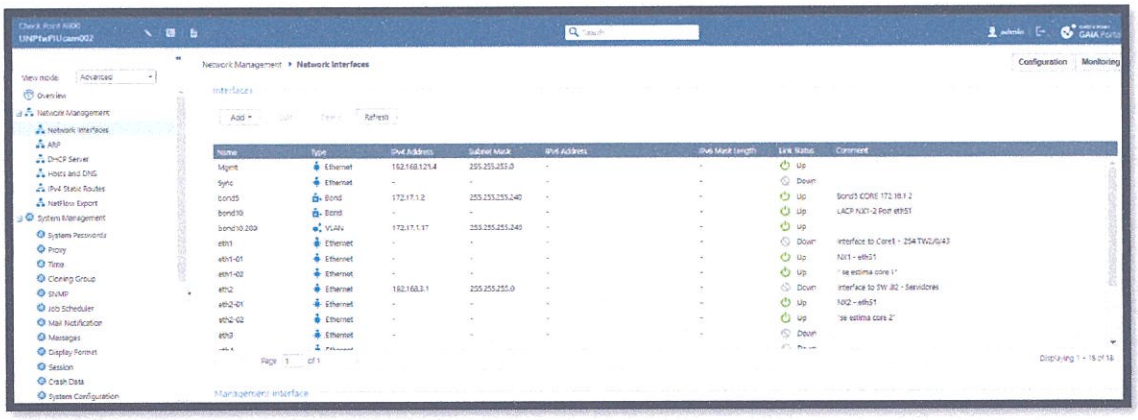
```
UNPfwPIUcam002> show installer packages installed
**  ********************************************************************************** **
**                                    Hotfixes                                        **
**  ********************************************************************************** **
Display name
                Type
R81.20 Jumbo Hotfix Accumulator Recommended Jumbo Take 65
                Hotfix
R81.20 Jumbo Hotfix Accumulator Recommended Jumbo Take 76
                Hotfix
R81.20 Take 53 Security hardening for Remote Access VPN users
                Package
**  ********************************************************************************** **
**                                   Blink Images                                     **
**  ********************************************************************************** **
Display name
                Type
<b>R81.20 Security Gateway + JHF T26 for Appliances and Open Servers</b>
                Blink Version
```

Por SSH 192.168.121.4 vemos los paquetes instalados

En esta imagen podemos corroborar con el comando ***"show installer packages installed"*** la validación de las últimas versiones instaladas recomendadas por el fabricante, asimismo manejamos una interfaz web con sistema operativo GAIA en donde realizamos dichas actividades por URL, mostramos ello.

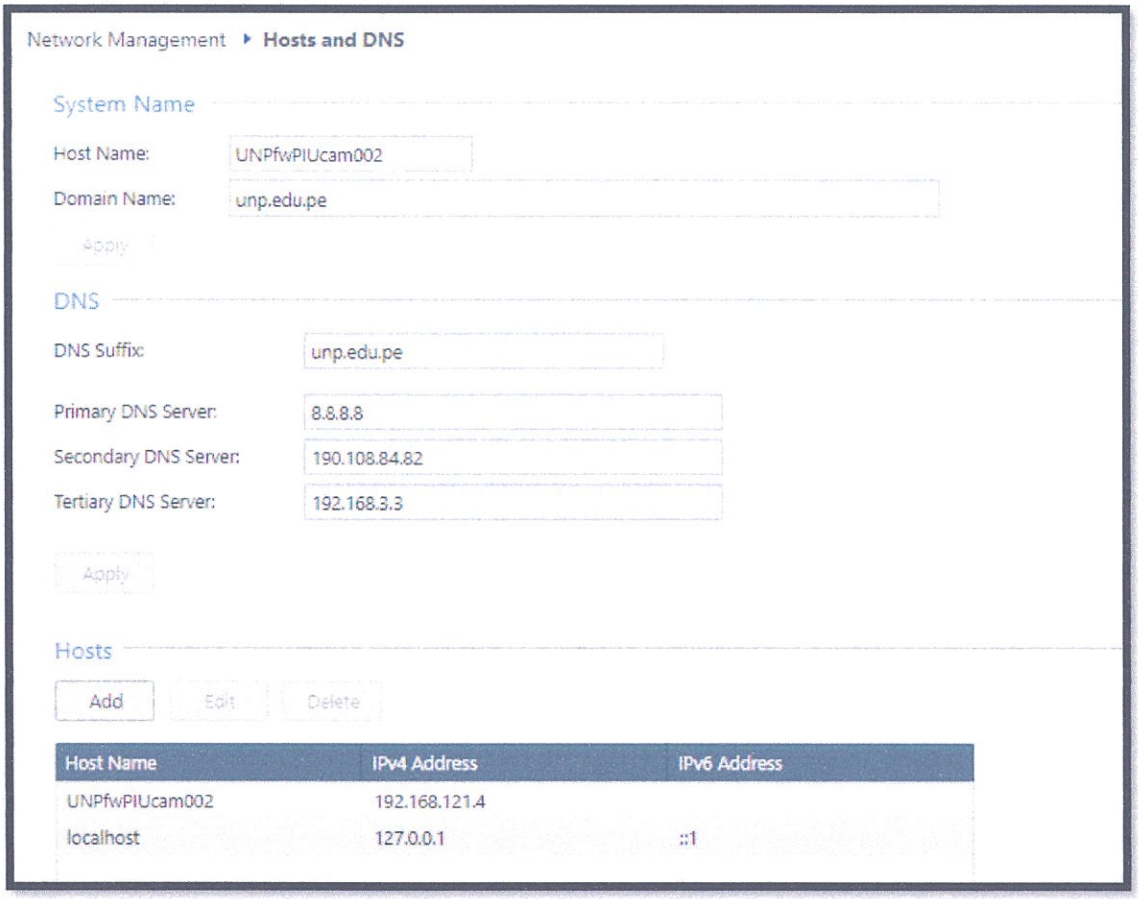


Muestra de la versión por el S.O Gaia manejado por web

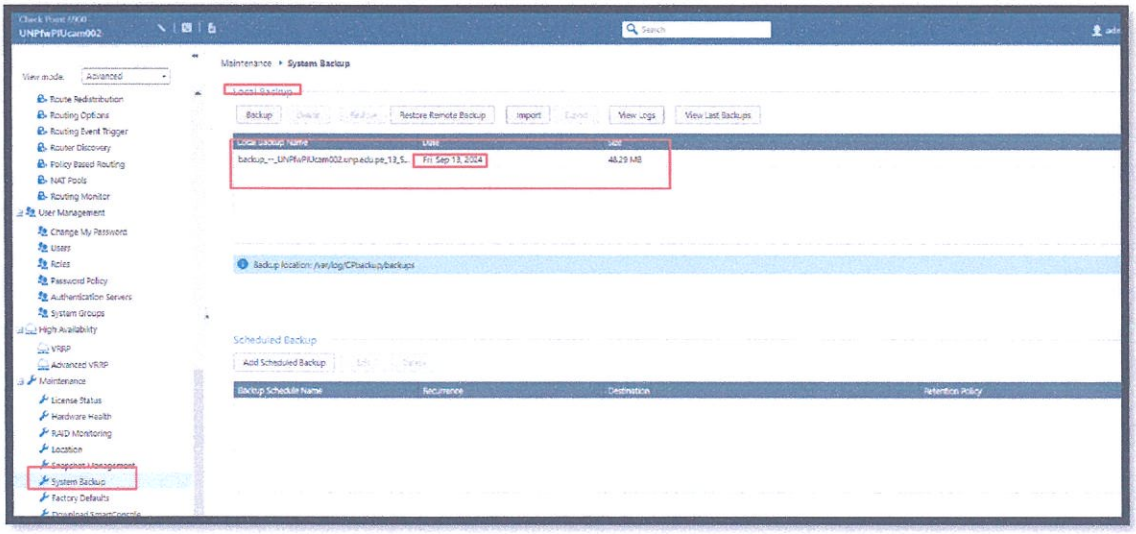


Vista de la configuración de las interfaces físicas

Aquí podemos ver la creación de interfaces virtuales para la conexión con los switches existentes NEXUS de cisco en la entidad, además de ello se crean más interfaces virtuales para mantener la conectividad con los CORE del DATA CENTER

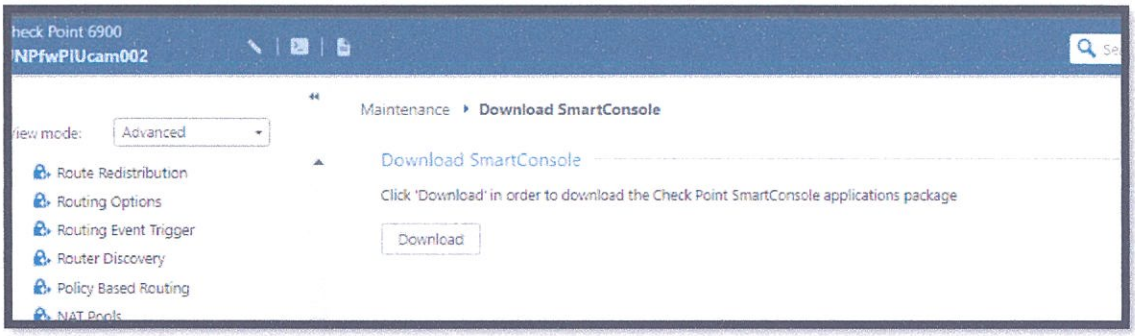


Configuración de DNS a través de la interfaz WEB



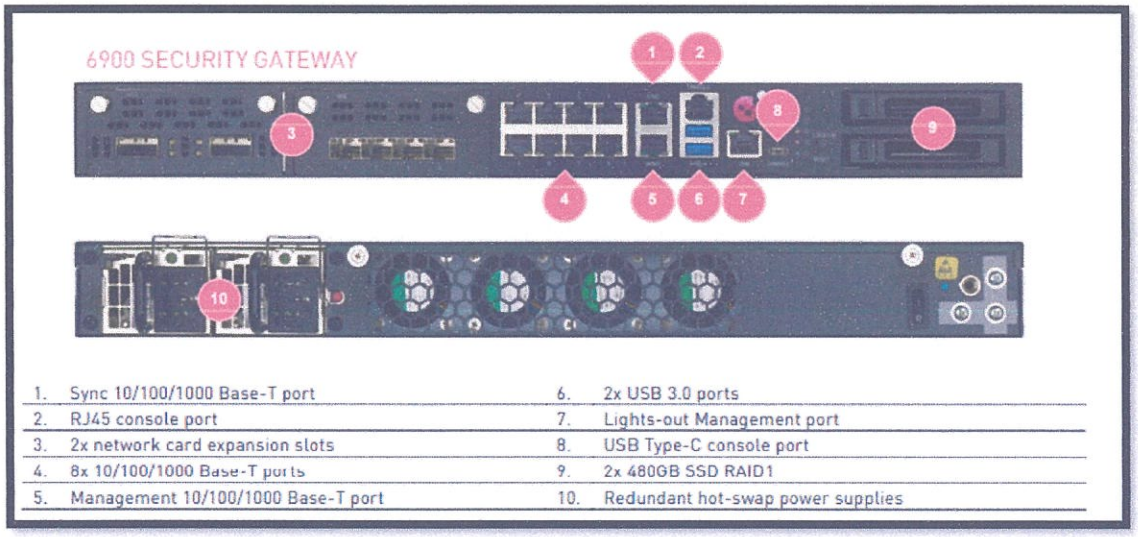
Gestión de backup , iniciándolo desde la web Gaia.

La ventaja de tener esa opción de realizar los backup y snapshots es que podemos exportarlo ya sea a un servidor de almacenamiento o directamente desde el punto de acceso donde iniciamos el equipo.



Apertura para la descarga del Software Smartconsole última versión recomendada.

Con esta actualización del producto podemos descargar todos los elementos básicos para la gestión y monitoreo de los equipos a la última versión, esto nos ayuda a que sea segura la descarga y eficiente.



1.	Sync 10/100/1000 Base-T port	6.	2x USB 3.0 ports
2.	RJ45 console port	7.	Lights-out Management port
3.	2x network card expansion slots	8.	USB Type-C console port
4.	8x 10/100/1000 Base-T ports	9.	2x 480GB SSD RAID1
5.	Management 10/100/1000 Base-T port	10.	Redundant hot-swap power supplies

Observamos los componentes del equipo con slots de F.O de 40 Gb

Ventajas de tener puertos de 40 gb

Principalmente por estas razones:

- **Mayor velocidad:** La principal ventaja es la velocidad de transferencia de datos, que es cuatro veces mayor que la de los puertos de 10 Gb. Esto es crucial para aplicaciones que demandan mucho ancho de banda, como:
    - **Centros de datos:** Donde se manejan grandes volúmenes de información y se requiere una conexión rápida entre servidores de la UNP.
    - **Redes Internas de la Universidad:** Para soportar aplicaciones de alta demanda como virtualización, almacenamiento en la nube y videoconferencia de alta calidad.
    - **Entornos de alta performance:** Donde se necesitan altas velocidades para procesar grandes cantidades de datos de manera rápida.
- **Menor latencia:** Además de la velocidad, los puertos de 40 Gb ofrecen una latencia más baja, lo que significa que los datos se transmiten con menor demora. Esto es fundamental para aplicaciones sensibles a la latencia, como las comunicaciones en tiempo real.
- **Escalabilidad:** Los puertos de 40 Gb permiten escalar las redes de manera más eficiente, ya que pueden soportar un mayor número de usuarios y aplicaciones sin comprometer el rendimiento.
- **Consolidación de tráfico:** Al ofrecer un mayor ancho de banda, los puertos de 40 Gb permiten consolidar múltiples conexiones en un solo enlace físico, lo que simplifica la gestión de la red y reduce costos.

VI. Especificaciones del NGXT 6900

SPECIFICATIONS

Performance

Enterprise Test Conditions	
Threat Prevention[1] (Gbps)	7.4
NGFW[2] (Gbps)	17
IPS (Gbps)	19
Firewall (Gbps)	37
RFC 3511, 2544, 2647, 1242 PERFORMANCE (LAB)	
Firewall 1518B UDP (Gbps)	63
VPN AES-128 (Gbps)	9.81
Connections/sec	230,000
Concurrent connections[3]	4/8/16M

1: Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection. 2: Includes Firewall, Application Control and IPS. 3: Performance measured with default/Plus/maximum memory.

Additional Features

Highlights
• 1x CPUs, 8 physical cores, 16 virtual cores
• 1x 480GB SSD storage (2x in Plus)
• 1 AC or DC power supply (2x in Plus)
• 16, 32 and 64 GB memory options
• Lights-Out-Management (included in Plus)
• Virtual Systems (Base/Plus/max mem): 10/20/20
Network Expansion Slot Options (2 of 2 slots open)
• 8x 10/100/1000Base-T RJ45 port card, up to 26 ports
• 4x 1000Base-F SFP port card, up to 8 ports
• 4x 10GBase-F SFP+ port card, up to 8 ports
• 2x 40GBase-F QSFP+ port card, up to 4 ports

Content Security

First Time Prevention Capabilities
• CPU-level, OS-level and static file analysis
• File disarm and reconstruction via Threat Extraction
• Average emulation time for unknown files that require full sandbox evaluation is under 100 seconds
• Maximal file size for Emulation is 100 MB
• Emulation OS Support: Windows XP, 7, 8.1, 10
Applications
• Use 8,000+ pre-defined or customize your own applications
• Accept, prevent, schedule, and apply traffic-shaping
Data Loss Prevention
• Classify 700+ pre-defined data types
• End user and data owner incident handling

Physical

Power Requirements

- Single Power Supply rating: 300W
- AC power input: 100 to 240V (47-63Hz)
- Power consumption avg/max: 139W/275W
- Maximum thermal output: 938 BTU/hr.

Dimensions

- Enclosure: 1RU
- Dimensions (WxDxH): 17.2 x 20 x 1.73 in. (438 x 508 x 44mm)
- Weight (Base/Plus): 17.6/19.8 lbs. (8.45/9 kg)

Environmental Conditions

- Operating: 0° to 40°C, humidity 95%
- Storage: –20° to 70°C, humidity 95%

Certifications

- Safety: UL, CB, CE, TUV GS
- Emissions: FCC, CE, VCCI, RCM/C-Tick
- Environmental: RoHS, WEEE, REACH[1], ISO14001[1]

Content Security (continued)

Dynamic User-based Policy

- Integrates with Microsoft AD, LDAP, RADIUS, Cisco pxGrid, Terminal Servers and with 3rd parties via a Web API
- Enforce consistent policy for local and remote users on Windows, macOS, Linux, Android and Apple iOS platforms

Network

Network Connectivity

- Total physical and virtual (VLAN) interfaces per appliance: 1024/4096 (single gateway/with virtual systems)
- 802.3ad passive and active link aggregation
- Layer 2 (transparent) and Layer 3 (routing) mode

High Availability

- Active/Active L2, Active/Passive L2 and L3
- Session failover for routing change, device and link failure
- ClusterXL or VRRP

IPv6

- NAT66, NAT64, NAT46
- CoreXL, SecureXL, HA with VRRPv3

Unicast and Multicast Routing (see SK98226)

- OSPFv2 and v3, BGP, RIP
- Static routes, Multicast routes
- Policy-based routing
- PIM-SM, PIM-SSM, PIM-DM, IGMP v2, and v3

Con el datasheet concluimos que ,Checkpoint **Quantum 6900** es una solución de seguridad de red de alto rendimiento diseñada para proteger a las empresas de las amenazas cibernéticas más sofisticadas. Con su potente combinación de hardware y software, este firewall ofrece una protección integral para redes de tamaño mediano a grande.

- **Rendimiento excepcional:** El 6900 ofrece un rendimiento de hasta 17 Gbps para inspección de tráfico de red, garantizando una protección sin comprometer la velocidad de su red.
- **Prevención de amenazas de día cero:** Gracias a la tecnología SandBlast, el 6900 detecta y bloquea amenazas desconocidas antes de que puedan causar daños, protegiendo su empresa contra ataques de día cero.
- **Escalabilidad:** El 6900 se adapta fácilmente a las necesidades cambiantes de su negocio, ofreciendo opciones de expansión para manejar el crecimiento de su red.
- **Gestión unificada:** Centralice la gestión de su seguridad de red con la plataforma de gestión unificada de Checkpoint, simplificando las operaciones y reduciendo los costos.
- **SD-WAN integrado:** Optimice sus conexiones de red y reduzca los costos con las capacidades de SD-WAN integradas en el 6900.

- **Protección de aplicaciones:** Identifique y proteja las aplicaciones empresariales críticas, asegurando la continuidad de su negocio.

VII. DESCRIPCION DEL BIEN A ESTANDARIZAR

El presente documento tiene por finalidad establecer el sustento técnico para la estandarización de todas las plataformas de ciberseguridad que se complementen con el firewall Checkpoint 6900 existente en la infraestructura de red de la Universidad Nacional de Piura (UNP).

Se detallan las soluciones requeridas a estandarizar:

- Proteción de CIBERSEGURIDAD para correo de nube.
- Protección con firewall virtuales para máquinas virtuales de nube
- Proteciín lateral: XDR, NDR

Rendimiento y escalabilidad: El NGTX Checkpoint 6900 ofrece un rendimiento excepcional y la capacidad de adaptarse a las crecientes demandas de la red universitaria, asegurando una protección óptima incluso en entornos de alta densidad de tráfico.

- **Amplio conjunto de características:** La plataforma Checkpoint proporciona un conjunto completo de funcionalidades de seguridad, incluyendo prevención de intrusiones, filtrado de contenido, protección contra malware y gestión de riesgos.
- **Integración con otros sistemas:** El Checkpoint 6900 se integra fácilmente con otros componentes de la infraestructura de seguridad de la UNP, como sistemas de detección de intrusos (IDS), sistemas de prevención de pérdida de datos (DLP) y soluciones de seguridad en la nube.
- **Experiencia y soporte:** Checkpoint cuenta con una larga trayectoria en el mercado de la seguridad de redes y ofrece un amplio soporte técnico y servicios profesionales.

Principales ventajas de la solución Checkpoint 6900:

- **Seguridad de última generación:** Protección proactiva contra amenazas conocidas y emergentes.
- **Visibilidad integral:** Monitoreo detallado del tráfico de red para detectar anomalías y responder rápidamente a incidentes.
- **Gestión simplificada:** Consola de gestión unificada para facilitar la administración de la seguridad en toda la red.
- **Alta disponibilidad:** Diseño redundante para garantizar la continuidad de las operaciones.
- **Flexibilidad:** Capacidad de adaptarse a las necesidades cambiantes de la UNP.

VIII. JUSTIFICACIÓN TÉCNICA

La estandarización del firewall Checkpoint 6900 en la UNP permitirá:

- ***Consolidar la seguridad:*** *Unificar las políticas de seguridad en una plataforma centralizada,* mejorando la eficiencia y reduciendo el riesgo de errores de configuración.
- **Simplificar la gestión:** Centralizar la administración de la seguridad en una única consola, lo que reduce la carga de trabajo del equipo de TI.
- **Optimizar los recursos:** Aprovechar al máximo las capacidades de los dispositivos Checkpoint, evitando la duplicación de funciones y optimizando el uso de los recursos.
- **Aumentar la resiliencia:** Crear una infraestructura de seguridad más robusta y resistente a las amenazas cibernéticas.
- **Facilitar la expansión:** Simplificar la expansión de la red y la incorporación de nuevos servicios.

IX. PLAN DE IMPLEMENTACIÓN

El plan de implementación incluirá las siguientes etapas:

- **Análisis de la infraestructura actual:** Evaluación detallada de la red existente para identificar los requisitos específicos y los puntos de integración.
- **Diseño de la arquitectura:** Diseño de una arquitectura de seguridad escalable y adaptable a las necesidades futuras de la UNP.
- **Implementación de los dispositivos:** Instalación y configuración de los firewalls Checkpoint 6900 en los puntos estratégicos de la red.
- **Integración con otros sistemas:** Conexión de los firewalls con otros sistemas de seguridad y aplicaciones.
- **Capacitación del personal:** Impartición de cursos de capacitación al personal técnico de la UNP.
- **Monitoreo y mantenimiento:** Monitoreo continuo del sistema para garantizar su correcto funcionamiento y provisión de servicios de mantenimiento.

La estandarización del firewall Checkpoint 6900 en la UNP representa una inversión estratégica para garantizar la seguridad de la infraestructura de red y proteger los valiosos activos informáticos de la institución. Esta solución ofrecerá una protección integral, simplificará la gestión de la seguridad y permitirá a la UNP enfrentar los desafíos de ciberseguridad actuales y futuros.

X. USO QUE SE LE DARÁ AL EQUIPAMIENTO DE CIBERSEGURIDAD A ESTANDARIZAR.

- Filtrado de tráfico: El firewall actuará como un guardián, permitiendo únicamente el tráfico autorizado hacia y desde los servidores que alojan las aplicaciones y bases de datos.
- Prevención de intrusiones: Detectará y bloqueará intentos de intrusión, como escaneos de puertos, exploits y ataques de fuerza bruta.
- Protección contra malware: Bloqueará el acceso de malware a los servidores, evitando la infección de sistemas y la pérdida de datos.

Seguridad de Aplicaciones

- Protección de aplicaciones web: El firewall protegerá las aplicaciones web de ataques como inyección SQL, XSS (Cross-Site Scripting), y otros tipos de vulnerabilidades comunes en aplicaciones web.
- Control de acceso basado en aplicaciones: Permitirá definir políticas de acceso granular para cada aplicación, asegurando que solo los usuarios autorizados puedan acceder a las funcionalidades específicas.
- Prevención de fuga de datos: Evitará la filtración de datos confidenciales al monitorear el tráfico de las aplicaciones y bloquear las transferencias no autorizadas.

Seguridad de Bases de Datos

- Protección de bases de datos: El firewall protegerá las bases de datos de ataques directos y de vulnerabilidades en las aplicaciones que acceden a ellas.
- Control de acceso a bases de datos: Definirá políticas de acceso precisas para cada base de datos, asegurando que solo los usuarios autorizados puedan realizar consultas y modificaciones.
- Prevención de exfiltración de datos: Evitará que los datos confidenciales almacenados en las bases de datos sean copiados o extraídos de forma no autorizada.

XI. JUSTIFICACIÓN DE LA ESTANDARIZACIÓN

La estandarización de una solución de ciberseguridad centralizada basada en la marca Checkpoint para la Universidad Nacional de Piura (UNP) representa una inversión estratégica para garantizar la integridad, confidencialidad y disponibilidad de los sistemas informáticos de la institución. A continuación, se presenta una justificación detallada de esta decisión:

CONSOLIDACIÓN DE LA SEGURIDAD:

- **Política de seguridad unificada:** Al utilizar una única plataforma de seguridad, se facilita la implementación de una política de seguridad coherente y centralizada en toda la infraestructura de la UNP.
- **Reducción de la complejidad:** La gestión de múltiples soluciones de seguridad aumenta la complejidad y el riesgo de errores de configuración. Con una solución unificada, la administración se simplifica considerablemente.

MEJORA DE LA EFICIENCIA:

- **Gestión centralizada:** Una consola de gestión unificada permite administrar todas las políticas de seguridad desde un solo punto, lo que ahorra tiempo y recursos.
- **Automatización de tareas:** Muchas tareas de gestión, como la creación de reglas de firewall y la generación de informes, pueden automatizarse, lo que reduce la carga de trabajo del equipo de seguridad.

MAYOR VISIBILIDAD:

- **Monitoreo integral:** Al tener todos los componentes de seguridad bajo una misma plataforma, se obtiene una visión consolidada del tráfico de red, lo que facilita la detección de amenazas y anomalías.
- **Generación de informes:** Se pueden generar informes detallados sobre el estado de seguridad de la red, lo que permite identificar tendencias y tomar decisiones basadas en datos.

FACILIDAD DE MANTENIMIENTO:

- **Capacitación simplificada:** El personal técnico solo necesita capacitarse en una única plataforma, lo que reduce los costos de capacitación y mejora la eficiencia.
- **Soporte técnico unificado:** El proveedor de la solución puede ofrecer un soporte técnico más eficiente y personalizado al tener una base de clientes más concentrada en un único producto.

ESCALABILIDAD:

- **Adaptación a las necesidades cambiantes:** La plataforma Checkpoint es altamente escalable, lo que permite adaptarse a las necesidades crecientes de la UNP sin necesidad de reemplazar todo el equipo.

REDUCCIÓN DE COSTOS:

- **Optimización de licencias:** Al utilizar una única solución, se pueden negociar mejores condiciones con el proveedor y optimizar el costo de las licencias.
- **Reducción de costos operativos:** La simplificación de la gestión y el mantenimiento reduce los costos operativos a largo plazo.

MEJORA DE LA RESPUESTA A INCIDENTES:

- **Detección temprana de amenazas:** Las características avanzadas de la plataforma Checkpoint permiten detectar amenazas de manera temprana, lo que reduce el tiempo de respuesta a incidentes.
- **Orquestación de la respuesta:** La solución puede integrarse con otros sistemas de seguridad para automatizar la respuesta a incidentes, lo que minimiza el impacto de los ataques.

CUMPLIMIENTO NORMATIVO:

- **Aseguramiento de la conformidad:** La solución Checkpoint ayuda a cumplir con las normativas de seguridad y privacidad aplicables, como el RGPD y la Ley de Protección de Datos Personales.

PROTECCIÓN DE LOS ACTIVOS DE LA INSTITUCIÓN:

- **Protección de la infraestructura crítica:** La solución protege los servidores, aplicaciones y bases de datos de la UNP de amenazas cibernéticas como malware, ransomware y ataques de denegación de servicio.

- **Garantía de la continuidad del negocio:** Al minimizar el riesgo de interrupciones en los servicios, la solución contribuye a garantizar la continuidad de las operaciones académicas y administrativas de la UNP.

XII. INCIDENCIA ECONÓMICA DE LA CONTRATACIÓN

PRODUCTO CHECKPOINT	CANTIDAD	Precio Incluido Impuestos
Appliance y Licencias del equipo NGTX Checkpoint 6900 (S/N 2028BA2098). Firewall, Ipsec, VPN, IPS, Control de aplicaciones, Content Awareness, Filtro, URL, Antivirus, Anitbot, Threat emulation cloud, Threat extraccion, Antispam y Email Security, Mobile Access	1	S/ 500,000.00

XIII. PERIODO DE VIGENCIA DE ESTANDARIZACIÓN

La estandarización requerida deberá tener una vigencia de tres (03) años, debiendo tener en cuenta que de variar la condiciones que determinaron la estandarización, se pondrá en conocimiento de la Dirección General y el Rectorado de la UNP, a fin de dejar sin efecto la estandarización requerida.

XIV. CONCLUSIÓN.

Con el fin de asegurar la continuidad de las operaciones, optimizar la gestión de la seguridad y proteger los valiosos activos informáticos de la UNP, se recomienda la estandarización de los firewalls de nueva generacion Checkpoint y sus derivados:

- Proteción de CIBERSEGURIDAD para correo de nube.
- Protección con firewall virtuales para máquinas virtuales de nube
- Proteciín lateral: XDR, NDR

Esta solución ofrecerá un alto nivel de seguridad, rendimiento y escalabilidad, permitiendo a la institución cumplir con sus objetivos estratégicos por un periodo de 3 años.