PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SUMINISTRO E INSTALACIÓN DE UN SISTEMA UNIFICADO DE COMUNICACIONES PARA TODA LA RED DE LA UNIVERSIDAD DE CANTABRIA (UNICAN)

OBJETO: Suministro e instalación de un sistema unificado de comunicaciones para toda la red de la Universidad de Cantabria (UNICAN).

DESCRIPCIÓN Y CARACTERÍSTICAS TÉCNICAS:

El objeto del contrato se articula en las siguientes áreas:

1. Infraestructura de comunicaciones:
    1.1. CORE y CPD
    1.2. Distribución /Concentración
    1.3. Acceso (Edge)
        1.3.1. Aulas/Salas
    1.4. WiFi
    1.5. Otro equipamiento
2. Seguridad perimetral
    2.1. UNICAN
    2.2. Aulas/Salas
    2.3. VPN-SSL
    2.4. Gestor de Ancho de Banda
3. Plataforma de gestión:
    3.1. Gestión de red
    3.2. Sistema de Control de Acceso (NAC)
4. Instalación y configuración.

5. Garantía .

6. Formación.

Todo el equipamiento, deberá ser redundante a nivel de procesamiento, control , conmutación y enrutamiento, para cada uno de los equipos de CORE, distribución/concentración, seguridad perimetral, control de accesos, monitorización y logs y WiFi.

Se suministrarán los latiguillos de fibra óptica necesarios en distancia y tipo de conectores requeridos para el correcto conexionado y funcionamiento de toda la infraestructura, junto con los adaptadores/atenuadores que requiera la oferta.

El equipamiento debe ser tal que, con todos los puertos requeridos ocupados con tarjetas de máxima capacidad posible y operando a "line-rate", no tenga sobresuscripción. Además, debe soportar el procesamiento de dicho tráfico, tanto entrante como saliente, sin que las prestaciones de los equipos se degraden. Estas condiciones deben, así mismo, cumplirse para el caso de completar el equipo con módulos, stack's adicionales hasta completar la máxima capacidad del sistema.

Los equipos propuestos deben soportar las funcionalidades requeridas para cualquier tipo de interfaz de las solicitadas o de las futuras interfaces que pudieran adquirirse.

1.- Infraestructura de comunicaciones:

Éste área abarca todos los dispositivos y servicios de mantenimiento de los equipos de comunicaciones LAN de la Universidad. Las características técnicas de los equipamientos serán iguales para todos, independiente de la finalidad del mismo, indicándose en algún caso parámetros mínimos que deben cumplir para cada área. Las características comunes son las siguientes:

- Soporte de módulos SFP y SFP+, capaces de soportar los puertos/transceivers:
    - Interfaces Ethernet 10/100/1000. Conectores UTP RJ-45.
    - 1000 Base-SX
    - 1000 Base-LX
    - 10GBase-SR
    - 10GBase-SRL
    - 10GBase-LR
    - 10G Base-LRM
    - 10GBase-CR

- Backplane non-blocking

- más de 7000 flujos por segundo y módulo para CORE y Distribución/Concentración.
- Todos los puertos funcionarán a velocidad de cable (Line rate)
- Equipos en formato de chasis/pila, de tamaño adecuado al número de enlaces y puertos a conectar.
- 110 to 240 V universal input N+1 o N+N redundancy
- Safety: UL 60950-1, FDA 21 CFR 1040.10 and 1040.11, CAN/CSAC22.2 No. 60950-1, EN 60950-1, EN 60825-1, EN 60825-2, IEC60950-1, 2006/95/EC (Low Voltage Directive)
- Electromagnetic compatibility: FCC 47 CFR Part 15 (Class A), ICES-003 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, EN61000-3-3, AS/NZ CISPR-22 (Class A). VCCI V-3. CNS 13438 (BSMI),2004/108/EC (EMC Directive)
- Reduction of Hazardous Substances (ROHS) 5/6
- Acoustic noise: 62 dBA (based on operational tests taken from bystander position [front] and performed at 23° C in compliance with ISO 7779)
- CSA 60950-1 (2003) Safety of Information Technology Equipment
- UL 60950-1 (2003) Safety of Information Technology Equipment
- EN 60950-1 (2001) Safety of Information Technology Equipment
- IEC 60950-1 (2001) Safety of Information Technology Equipment (with country deviations)
- EN 60825-1 +A1+A2 (1994) Safety of Laser Products— Part 1: Equipment Classification
- EN 60825-2 (2000) Safety of Laser Products—Part 2: Safety of Optical Fiber Comm. Systems
- C-UL to CAN/CSA 22.2 No.60950-1(First Edition)
- TUV/GS to EN 60950-1, Amendment A1-A4, A11
- CB-IEC60950-1
- EN 300 386 V1.3.3 (2005) Telecom Network Equipment—EMC requirements
- FCC Part 15 Class A (2007) USA Radiated Emissions
- EN 55022 Class A (2006) European Radiated Emissions
- ICES-003 Class A
- AS/NZS CISPR 22 Class A

- CISPR 22 Class A
- EN 55024 +A1+A2 (1998) Information Technology Equipment Immunity Characteristics
- EN-61000-3-2 (2006) Power Line Harmonics
- EN-61000-3-3 +A1 +A2 +A3 (1995) Power Line Voltage Fluctuations
- EN-61000-4-2 +A1 +A2 (1995) Electrostatic Discharge
- EN-61000-4-3 +A1+A2 (2002) Radiated Immunity
- EN-61000-4-4 (2004) Electrical Fast Transients
- EN-61000-4-5 (2006) Surge
- EN-61000-4-6 (2007) Immunity to Conducted Disturbances
- EN-61000-4-11 (2004) Voltage Dips and Sags
- GR-63-Core (2006) Network Equipment, Building Systems (NEBS) Physical Protection
- GR-1089-Core (2006) EMC and Electrical Safety for Network Telecommunications Equipment
- SR-3580 (1995) NEBS Criteria Levels (Level 3)
- VLAN Registration Protocol (GVRP)
- 802.3ad – Link Aggregation Control Protocol (LACP)
- 802.1D – Spanning Tree Protocol
- 802.1w – Rapid Spanning Tree
- 802.1s – Multiple Instance Spanning Tree
- 802.3u Fast Ethernet
- 802.3ab Gigabit Ethernet (copper)
- 802.3z Gigabit Ethernet (fiber)
- 802.3ae 10 Gigabit Ethernet (fiber)
- 802.1Q VLANs
- 802.3x Flow Control
- Soporte para Jumbo frames (9216 bytes) with MTU Discovery Support for Gigabit

- Link Flap Detection
- Dynamic Egress (Automated VLAN Port Configuration)
- 802 1ab LLDP-MED
- 802.3 ah
- RFC 1256 ICMP Router Discovery Protocol
- RFC 826 ARP
- RFC 1027 Proxy ARP
- Static Routes
- RFC 1058 RIPv1
- RFC 1723 RIPv2 with Equal Cost Multipath Load Balancing
- RFC 1812 RIP Requirements
- RFC 1519 CIDR
- RFC 2338 Virtual Router Redundancy Protocol (VRRP)
- DHCP Server RFC 1541/ Relay RFC 2131
- RFC 1583/RFC 2328 OSPFv2
- RFC 1587 OSPFv2 NSSA
- RFC 1765 OSPF Database Overflow
- RFC 2154 OSPF with Digital Signatures (Password & MD5)
- OSPF with Multipath Support
- OSPF Passive Interfaces
- IPv6 Routing Protocol
- RFC 3031 Multiprotocol Label Switching
- RFC 1701 Generic Routing Encapsulation
- Extended ACLs
- Policy-based Routing

- RFC 1112 IGMP
- RFC 2236 IGMPv2
- RFC 3376 IGMPv3
- DVMRP v3-10
- Static routing
- Filter-based forwarding
- IPv6
- Bidirectional Forwarding Detection (BFD)
- VRF Virtual Routing and Forwarding (Ready)
- Ingress & egress L2-L4 access control lists (ACLs):
  .- Port ACLs
  .- VLAN ACLs
  .- Router ACLs
- Web-based Authentication
- MAC-based Authentication
- Multiple Authentication Types per Port Simultaneously
- Multiple Authenticated users per Port with unique policies per user/End System (VLAN association independent)
- RFC 3580 IEEE 802.1 RADIUS Usage Guidelines, with VLAN to Policy Mapping
- Worm Prevention (Flow Set-Up Throttling)
- Broadcast Suppression
- ARP Storm Prevention
- MAC-to-Port Locking
- Span Guard (Spanning Tree Protection)
- Behavioral Anomaly Detection/Flow Collector (non-sampled Netflow)
- Static Multicast Group Provisioning

- Multicast Group, Sender and Receiver Policy Control Class of Service
- Strict Priority Queuing
- Weighted Fair Queuing with Shaping
- IP ToS/DSCP Marking/Remarking
- IGMP snooping v1/v2/v3
- Protocol Independent Multicast PIM-SM, PIM-SSM, PIM-DM, MSDP
- LCD panel
- Extensive MIB support
- Queues per port: 8
- Policers: 2,000 per chassis
- Tabla de direcciones (MAC) Addresses, mínimo de 160.000 para CORE y Distribución/Concentración
- Mínimo de VLANs: 4.096
- Firewall filters (ACLs–Security and QoS)
- Link aggregation group (LAG) (ports/groups): 12/255
- Web-based Management Interface (http/https)
- Industry Common Command Line Interface
- Soporte de múltiples imágenes de software y configuraciones, con capacidad de revisión y vuelta atrás a cargar cualquiera (roll back).
- Multi-configuration File Support
- Editable Text-based Configuration File
- COM Port Boot Prom and Image Download via ZMODEM
- Secure Shell (SSHv2) Server and Client
- FTP Client
- Netflow version 5 and version 9
- RFC 2865 RADIUS

- RFC 2866 RADIUS Accounting
- Management VLAN
- RFC 1156/1213 & RFC 2011 IP-MIB
- RFC 1493 Bridge MIB
- RFC 1659 RS-232 MIB
- RFC 1724 RIPv2 MIB
- RFC 2578 SNMPv2 SMI
- RFC 2579 SNMPv2-TC
- RFC 3417 SNMPv2-TM
- RFC 3418 SNMPv2 MIB
- RFC 2012 TCP MIB
- RFC 2013 UDP MIB
- RFC 2096 IP Forwarding Table MIB
- RFC 3411 SNMP Framework MIB
- RFC 3412 SNMP-MPD MIB
- RFC 3413 SNMPv3 Applications
- RFC 3414 SNMP User-Based SM MIB
- RFC 2276 SNMP-Community MIB
- RFC 2613 SMON MIB
- RFC 2674 802.1p/Q MIB
- RFC 2737 Entity MIB
- RFC 2787 VRRP MIB
- RFC 2819 RMON MIB (Groups 1-9)
- RFC 3273 HC RMON MIB
- RFC 2863 IF MIB

- RFC 2864 IF Inverted Stack MIB
- RFC 3291 INET Address MIB
- RFC 3621 Power Ethernet MIB
- RFC 3415 SNMP View Based ACM MIB
- RFC 3635 EtherLike MIB
- RFC 3636 MAU MIB
- IEEE 8023 LAG MIB
- RSTP MIB
- USM Target Tag MIB
- U Bridge MIB
- Draft-ietf-idmr-dvmrp-v3-10 MIB
- Draft-ietf-pim-sm-v2-new-09 MIB
- SNMP-REARCH MIB
- IANA-address-family-numbers MIB
- IEEE 802.1PAE MIB
- RFC 1155: Structure of Management Information (SMI)
- RFC 1157: SNMPv1
- RFC 1905, RFC 1907: SNMP v2c, SMIv2 and Revised MIB-II
- RFC 2570–2575: SNMPv3, user based security, encryption and authentication
- RFC 2576: Coexistence between SNMP Version 1, Version 2 and Version 3
- RFC 1212, RFC 1213, RFC 1215: MIB-II, Ethernet-like MIB and traps
- RFC 2925: Ping/Traceroute MIB
- RFC 2665: Ethernet-like interface MIB
- RFC 1643: Ethernet MIB
- RFC 2011: SNMPv2 for internet protocol using SMIv2

- RFC 2863: Interface MIB
- RFC 2932: IPv4 Multicast MIB
- RFC 1850: OSPFv2 MIB
- RFC 1657: BGP-4 MIB
- RFC 2287: System Application Packages MIB
- RFC 4188: STP and Extensions MIB
- RFC 4363: Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and VLAN extensions
- RFC 2922: LLDP MIB
- Draft-ietf-idr-bgp4-mibv2-02.txt: Enhanced BGP-4 MIB
- Draft-ietf-isis-wg-mib-07
- Draft-blumenthal-aes-usm-08
- Draft-reeder-snmpv3-usm-3desede-00
- Draft-ietf-idmr-igmp-mib-13
- Draft-ietf-idmr-pim-mib-09
- Draft-ietf-bfd-mib-02.txt
- Weighted Random Early Drop (WRED) scheduling
- Shaped Deficit Weighted Round Robin (SDWRR) queuing
- Multi-field classification (L2 – L4) for scheduling and rewrite
- RFC 1122: Host Requirements
- RFC 768: UDP
- RFC 791: IP
- RFC 783: Trivial File Transfer Protocol (TFTP)
- RFC 792: Internet Control Message Protocol (ICMP)
- RFC 793: TCP

- RFC 894: IP over Ethernet
- RFC 903: RARP
- RFC 906: TFTP Bootstrap
- RFC 2068: HTTP server
- RFC 1519: Classless Interdomain Routing (CIDR)
- RFC 1256: IPv4 ICMP Router Discovery (IRDP)
- RFC 2453: RIP v2
- RFC 1492: TACACS+
- RFC 2138: RADIUS Authentication
- RFC 2139: RADIUS Accounting
- RFC 2267: Network Ingress Filtering
- RFC 2030: Simple Network Time Protocol (SNTP)
- RFC 854: Telnet client and server
- RFC 951, 1542: BootP
- RFC 2131: BOOTP/Dynamic Host Configuration Protocol (DHCP) relay agent and DHCP server
- RFC 1591: Domain Name System (DNS)
- RFC 2328: OSPF v2 (Edge-mode)
- RFC 1765: OSPF Database Overflow
- RFC 2370: OSPF Opaque LSA Option
- RFC 3623: OSPF Graceful Restart
- RFC 2362: PIM-SM (Edge-mode)
- PIM-DM Draft IETF PIM: Dense Mode draft-ietf-idmr-pim-dm-05.txt, draft-ietf-pim-dm-new-v2-04.txt
- RFC 3569: Draft-ietf-ssm-arch-06.txt PIM-SSM PIM Source Specific Multicast
- RFC 1771: Border Gateway Protocol 4

- RFC 1965: Autonomous System Confederations for BGP
- RFC 2796: BGP Route Reflection (supersedes RFC 1966)
- RFC 1997: BGP Communities Attribute
- RFC 1745: BGP4/IDRP for IP-OSPF Interaction
- RFC 2385: TCP MD5 Authentication for BGPv4
- RFC 2439: BGP Route Flap Damping
- RFC 2918: Route Refresh Capability for BGP-4
- RFC 3392: Capabilities Advertisement with BGP-4
- RFC 4360: BGP Extended Communities Attribute
- RFC 4486: Subcodes for BGP Cease Notification message
- RFC 1195: Use of Open Systems Interconnection (OSI) IS-IS for Routing in TCP/IP and Dual Environments (TCP/IP transport only)
- RFC 2474: DiffServ Precedence, including 8 queues/port
- RFC 2598: DiffServ Expedited Forwarding (EF)
- RFC 2597: DiffServ Assured Forwarding (AF)
- RFC 2475: DiffServ Core and Edge Router Functions
- Out-of-band management: Serial; 10/100/1000BASE-T Ethernet
- Rescue configuration
- Image rollback
- RMON (RFC 2819) Groups 1, 2, 3, 9
- Network Time Protocol (NTP)
- DNS resolver
- Syslog logging
- Environment monitoring
- Temperature sensor

- Config-backup via FTP/secure copy
- Debugging: CLI via console, Telnet or SSH
- Diagnostics: Show, debug, and statistics commands
- Analyzer session: Ingress and/or egress traffic on multiple source ports monitored to one destination port or VLAN
- Local port and remote VLAN analyzers (up to seven sessions)
- IP tools: Extended ping and trace
- 802.1X authentication:
  • MAC authentication.
  • Web-based authentication (Port Web Authentication -PWA)), a where a user name and password are supplied through a browser
  • CEP, Convergence End Point, where multiple vendors VoIP phones are identified and authenticated.

  - Soporte de 1.024 usuarios/dispositivos por módulo, sin restricción del número de usuarios por puerto.
  - 9000 usuarios autenticados por chasis o similar para el CORE y Distribución/Concentración
- Power over Ethernet (PoE) Specifications

  • IEEE 802.3af
  • IEEE 802.3at para el acceso
  • Soporte de dispositivos PoE:
    - Class 1 (4 W)
    - Class 2 (7.5 W)
    - Class 3 (15.4 W)

  • El equipo, totalmente ocupado puede alimentar a dispositivos PoE de Class 3 en todos los puertos simultáneamente.
  •Distribución de alimentación Poe de forma manual o automática
  •Capacidad de control por puerto de:
    - Activar/desactivar
    - nivel de potencia eléctrica
    - priority safety
    - Sobrecarga (overload)

- Protección contra cortocircuitos

• Gestión eléctrica del sistema

- Passive chassis backplane or Meshed backplane architecture
- Hot swappable fan trays with multiple cooling fans
- Separate system and PoE power supplies
- Hot swappable power supplies
- Multiple AC input connections for power circuit redundancy
- Load sharing/redundant I/O fabrics
- N+1 fabric redundancy
- Hot swappable I/O fabrics and I/O modules
- Multiple host CPU's for N+X redundancy dynamic service fail-over, automatic module self-configuration, and multi-image support o similar
- NetFlow - Provides real-time visibility, application profiling, and capacity planning
- NAT - Network Address Translation
- LLDP-MED - Link Layer Discovery Protocol for Media Endpoint Devices enhances VoIP deployments
- Flow Setup Throttling - (FST) effectively preempts and defends against DoS attacks
- Web Cache Redirect - Increases WAN and Internet bandwidth efficiency
- Node & Alias Location - Automatically tracks user and device location and enhances network management productivity and fault isolation
- Port Protection Suite - Maintain network availability by ensuring good protocol and end station behavior

• Flex-Edge Technology - Provides advanced bandwidth management and allocation for demanding access/edge devices

- Multi-layer packet classification - enables the delivery of critical applications to specific users via traffic awareness and control

• User, Port, and Device Level (Layer 2 through 4 packet classification)
• QoS mapping to priority queues (802.1p & IP ToS/ DSCP) up to 16 queues per port
• Multiple queuing mechanisms (SPQ, WFQ, WRR, and Hybrid)
• Granular QoS/rate limiting
• VLAN to policy mapping

- Switching/VLAN services - provides high performance connectivity, aggregation, and rapid recovery services

  • Extensive industry standards compliance (IEEE and IETF)
  • Inbound and outbound bandwidth rate control per flow
  • VLAN services support
    - Link aggregation (IEEE 802.3ad)
    - Multiple spanning trees (IEEE 802.1s)
    - Rapid reconfiguration of spanning tree (IEEE 802.1w)
  • Flow setup throttling
- Distributed IP Routing - provides dynamic traffic optimization, broadcast containment, and more efficient network resilience

  • Standard routing features include static routes, OSPF v1/v2, RIPv1/RIPv2, IPv4, Policy Based Routing and Route Maps, and VRRPand Multicast routing support (DVMRP, IGMP v1/v2/v3, PIM-SM),
  • Extended ACLs
  • User security
    - Authentication (802.1X, MAC and PWA+, CEP), MAC (Static and Dynamic) port locking
    - Multi-user authentication/policies
  • Network security
    - Access Control Lists (ACL) – basic and extended
    - Policy-based security services (examples: spoofing, unsupported protocol access, intrusion prevention, DoS attacks limits)
  • Management Security
    - Secure access to the S-Series via SSH, SSL, SNMP v3
    - SNMP v1/v2c/v3, RMON (9 groups), and SMON (rfc2613) VLAN and Stats
    - Port/VLAN mirroring (one-to-one, one-to-many, many-to-many)
    - Unsampled NetFlow on every port with no impact on system switching and routing performance.

Todo el equipamiento ofertado, deberá funcionar bajo el mismo sistema operativo y versión, conservando varias configuraciones almacenadas para ser recuperadas y totalmente operativas cuando se necesite. La versión del sistema operativo que incluirá el equipo será la más actualizada y estable que exista en el momento del suministro, la cual implementará todas las funcionalidades especificadas en el presente pliego. También se incluirán todas aquellas licencias que fueran necesarias para utilizar dichas funcionalidades.

Se requiere la redundancia de las tarjetas procesadoras o en los stacks.

Se requiere que los equipos ofertados puedan instalarse en un rack estándar de 19" y 600mm de fondo contando las longitudes de las diferentes conexiones(datos, eléctricas,…) tanto frontales como traseras.
Tipo de alimentación eléctrica será AC 220V - 50Hz (redundante).
Se requiere redundancia de fuente de alimentación.

Los dispositivos de red son parte integral de la arquitectura de seguridad, por ello es necesario que implementen mecanismos que les protejan de ataques de DoS habituales como:

- TCP/UDP Port Scan
- Christmas Tree Attack
- Fraggle Attack
- Fragmented & Large ICMP
- ICMP Flood
- Invalid ICMP Attacks
- ICMP Re-Direct Attack
- LANd
- TCP Syn Fin Attack
- TCP Syn Flood
- Tear Drop Attack
- UDP Port Flood
- Invalid UDP Attacks
- Invalid IGMP Attacks
- Cisco Global Exploiter
- Shadowcode TTL Attack
- NTP DoS
- Open TCP Session Attacks
- Flood TCP Session

Para todos los enlaces de fibra óptica, se deberá estudiar y analizar el tipo de interface a instalar en los equipos junto con los dispositivos necesarios para que dicho enlace funcione a la máxima capacidad de la forma más eficiente, por lo tanto se suministrarán los atenuadores o amplificadores si fueran necesarios.

La red estará compuesta de las capas: acceso, distribución, CORE/CPD. Dependiendo del tamaño del

edificio considerado, se podrán colapsar las capas de acceso y distribución de edificio en una sola.

1.1 CORE y CPD:

La Universidad de Cantabria, dispone de 2 centros de procesos de datos, denominados "CPD Principal" y "CPD Réplica", los cuales se encuentran en edificios distintos y conectados por enlaces de fibra óptica extremo a extremo, de 500 mts. de distancia y fibra óptica monomodo de 9/125µ, tipo OS1, terminadas en bandejas con conectores tipo SC.

Desde ambos CPD, existen conexiones en fibra óptica monomodo, OS1, a todos los centros de distribución, por lo que se requieren, como mínimo, conexiones en 10Gb Ethernet entre ambos CPD y los edificios distribuidores. En caso de aumentar el número de enlaces, deberá ser igual el aumento para todos ellos.

Para cada uno de los CPD se suministrará un equipo switch/router de altas prestaciones y funcionalidades, que denominaremos CORE1 y CORE2 respectivamente. Los equipos deben ser idénticos, con todo el plano de control, procesamiento, fuentes de alimentación, ventilación, puertos de enlace redundantes y cumpliendo las características del presente pliego. Los equipos deberán soportar el estándar IEEE 802.3ba de 40Gb y 100Gb. En resumen, los equipos soportarán los siguientes protocolos de routing y transporte: RIP, OSPF, BGP, Multicast en todas sus versiones, IPv4/v6, MPLS.

En cada uno de los CPD's, se instalarán conmutadores/encaminadores en cada uno de los rack's que se disponen, conectados a los router-switch de "Core", cada uno de ellos con 2 enlaces 10Gbit-Ethernet mínimo, suministrando los latiguillos de fibra necesarios, para adoptar el modelo denominado "Top on Rack" en cada uno de los CPD's. Todas las conexiones de los conmutadores, serán como mínimo dobles al equipo de core y a placas/módulos diferentes. Los interfaces de conexión a los equipos de core, se realizará con interfaces del tipo "SFP+" de la velocidad requerida. Los equipos dispondrán al menos de 48 puertos 1000 Base-Tx a velocidad de cable (line rate) sin sobresuscripción.

CPD Principal: 9 Rack's de sala, distancias inferiores a 20 mts. al Core1

CPD Réplica: Hay un total de 20 Rack's de sala, con distancias inferiores a 20 mts. al Core2. En éste caso la conexión de esos 20 rack's se hará de la siguiente forma:

- 15 rack's se conectarán a otro conmutador/encaminador que se deberá suministrar, de igual características, funcionalidades y rendimientos al de los CORE, para realizar la conexión de los 15 Rack's en las mismas condiciones y características que el resto, mediante 2 enlaces de 10Gb a placas/slots diferentes del equipo destino. Éste equipo conmutador/enrutador, se conectará por enlace de fibras monomodo, con doble camino mínimo de 10Gb, hasta el equipo de concentración/acceso denominado D3 en placas/slots diferentes.

- Los 5 rack's restantes, se conectarán en las mismas condiciones técnicas al equipo de core del CPD réplica, mediante mínimo 2 enlaces de 10Gb a placas/slots diferentes.

En el CPD Principal se deberá suministrar un dispositivo router/switch, de las mismas funcionalidades, servicios, prestaciones y rendimientos que los detallados anteriormente y con las conexiones necesarias,

que se encargue de la conexión con el ISP de acceso a Internet y “balancee” el tráfico hacia el sistema de cortafuegos (2 equipos).

A nivel lógico, todo el equipamiento de comunicaciones instalado en ambos CPD, deberá comportarse como un único CPD o router central, no admitiéndose dispositivos intermedios o finales que realicen funciones de “alta disponibilidad”(HA) o similar. Se utilizarán tecnologías tipo “Virtual Chassis”, “Chassis Bonding”, “Virtual Switching System” o similares, de tal forma que la tecnología permita que 2 equipos al menos funcionen como una sola unidad lógica. Se deberá definir dicho recurso o técnica. Toda la información y documentación relacionada con la tecnología de los suministros ofertados, deberá incluirse, como se indica en el Anexo I.

Se suministrarán el número de enlaces necesarios para dar conexión completa a todos los dispositivos, tanto de comunicaciones como de seguridad que se requieren en el presente pliego, siempre teniendo en cuenta, que cuando se conecten 2 ó más enlaces a un mismo dispositivo, éstos terminarán en slots/módulos diferentes en ambos extremos.

Ambos CPD funcionarán simultáneamente y en caso de parada de uno de ellos, todo el sistema será capaz de trabajar a pleno rendimiento, sin disrupciones en el servicio y aplicaciones, se deberá indicar, explicar y garantizar dicho funcionamiento como se indica en el Anexo I.

Existen 8 edificios de distribución, que deberán estar conectados por caminos directos en fibra hacia ambos CORE. Se dispone de otros 5 edificios distribuidores, pero que no van conectados a los CORE, sino a equipos existentes del tipo JUNIPER M120 con interfaces 1 Gigabit-SX, que deberán conectarse por dos enlaces a dichos equipos. En caso de aumentar el número de enlaces para éste caso, se suministrarán las placas, interfaces, puertos,…, necesarios para realizar dicho enlace en todos y cada uno de los nodos D9 a D13, siendo el número igual para todos ellos.

El esquema de red propuesto aparece en las figuras: 1, 2, 3 y 4

1.2 Distribución/Concentración

Para esta capa, hay que tener en cuenta que los equipos además de realizar dicha función, en algunos casos también disponen de la capa de acceso, ya que se conectan usuarios finales directamente a dichos equipos. Existen 8 nodos (D1 a D8 de las figuras 1 y 2) de éste tipo que deberán conectarse al menos por un camino de fibra monomodo tipo OS1 a cada uno de los CORE, descritos anteriormente. Así mismo deberán concentrar/distribuir los enlaces a los nodos de acceso de cada edificio o edificios aledaños. La conexión con cada uno de los nodos de acceso del edificio se realizará, al menos por un camino de fibra multimodo tipo OM1 a velocidad de 10Gigabit Ethernet con conectores SFP+. Si el licitador propone aumentar el número de enlaces de los nodos de acceso del edificio, deberán conectarse a placas/slots diferentes del nodo de distribución con las mismas condiciones técnicas que las expresadas anteriormente, el número será igual para todos los armarios de acceso.

Los equipos deben tener las mismas características técnicas que las indicadas en el apartado a tal efecto. Los equipos se instalarán en rack’s estándar de 19”, con 600 mm de fondo contando las longitudes de las diferentes conexiones(datos, eléctricas,…) tanto frontales como traseras. Alimentación eléctrica

redundante

En la figura 6, se muestra el esquema de red propuesto, detallando tanto el mínimo de número de enlaces como de puertos de acceso para cada nodo.

1.3 Acceso (Edge):

Para ésta capa, los equipos, igual que en las anteriores, deben cumplir las características técnicas descritas en el apartado 1., añadiendo principalmente, la alta densidad de puertos de acceso en 1000Base-T que deben disponer y contar con capacidad de ampliación de al menos el 50 % de lo requerido. Si el licitador propone aumentar el número de enlaces de nodo de acceso del edificio al de concentración, deberán conectarse a placas/slots diferentes del nodo de concentración con las mismas condiciones técnicas que las expresadas anteriormente. El número de enlaces será igual para todos ellos.

La densidad de puertos para cada armario se puede ver en la figura 6; en las figuras 5 y 6 se muestra el esquema de red global propuesto desde el punto de vista físico y lógico.

Los equipos se instalarán en rack's estándar de 19", con 600 mm de fondo contando las longitudes de las diferentes conexiones(datos, eléctricas,…) tanto frontales como traseras.

El equipamiento de cada armario, se suministrará con al menos 8 puertos 1000 Base-T con estándar "IEEE 802.3at".

1.3.1 Aulas/salas

Se deberá suministrar un total de 60 equipos de 48 puertos de triple velocidad más 4 puertos con interfaces SFP y/o SFP+ y con 1 transceiver 10/100/1000 en RJ45 para cada uno de los equipos, que realizará el enlace al punto que suministre el Servicio de Informática, de las mismas características que los de CPD's, que dará servicio a las diferentes aulas y salas que dispone la universidad. Los cuales deben incorporarse en el sistema de seguridad y control de acceso que se detalla en el apartado 3. Los equipos se instalarán en rack's estándar de 19", con 600 mm de fondo contando las longitudes de las diferentes conexiones(datos, eléctricas,…) tanto frontales como traseras.

1.4 WiFi

La Universidad de Cantabria dispone de una red WiFi distribuida por todos los edificios pertenecientes a la institución, formada por 200 puntos de acceso de los modelos:

- 180 Cisco AP 1100 b/g
- 20 Cisco AP 1240 a/b/g con antenas AIR-ANT2465P-R y AIR-ANT2506

El modo de funcionamiento es el de "inteligencia" en el AP, con gestión centralizada mediante appliance WLSE de Cisco en la modalidad "Puntos de Acceso Inteligentes(autónomos)" . Todos los AP están instalados y conectados con "power injector", dispositivo "antivandálico" con llave maestra. Dicha red ha demostrado su fiabilidad, rendimiento, estabilidad y capacidad de funcionamiento. Lo que se solicita es el cambio de modalidad de funcionamiento a "puntos de acceso ligeros" con controladores de LAN inalámbrica. El cambio deberá ser capaz de soportar las gestión de todos los AP simultáneamente con un mínimo de 250;

todo el equipamiento ofertado deberá serlo en alta disponibilidad y redundancia, para albergar cada uno de ellos, como mínimo en cada Core, así mismo, en caso de caída de uno de los equipos, el otro será capaz de gestionar en las mismas condiciones técnicas todos los puntos de acceso. En caso de sustituir los puntos de acceso actuales por otros, se deberá detallar el modelo y características en la documentación adicional solicitada en el Anexo I, exigiendo que a las características actuales de los puntos de acceso, deban cumplir el estándar 802.11n; también se deberá realizar la sustitución de los equipos actuales por personal propio de la empresa y manteniendo la distribución, salvo que se presente un estudio de coberturas realizado con herramientas especializadas que justifique su cambio; en tal caso la empresa correrá con los gastos ocasionados. Todas las intervenciones, configuraciones,…, serán supervisadas y aprobadas por el Servicio de Informática. Las características de los equipos nuevos deberán ser igual o superior a las de los equipos actuales.

1.5 Otro equipamiento

Para cada uno de los armarios de comunicaciones que existen y se detallan en el presente pliego, apartados 1.1, 1.2 y 1.3, salvo para los 2 denominados CPD, se suministrará equipos de alimentación ininterrumpida (SAI/UPS) del tipo ON-line, con una capacidad de potencia del 50% adicional a la que se obtenga de la suma de las potencias de los dispositivos que se instalen en cada rack individualmente, con un tiempo de suministro off-line, no inferior a 20 minutos. Los equipos dispondrán de tarjeta de red Ethernet, gestionable tanto por el estándar SNMP en todas sus versiones, como software/aplicación de gestión centralizada que esté totalmente integrada en la plataforma de gestión de red que se describe en este pliego apartado 3. Los equipos se instalarán en rack's estándar de 19" con 600 mm de fondo contando las longitudes de las diferentes conexiones (datos, eléctricas,…) tanto frontales como traseras y no podrán ocupar más de 3 U.

2.- Seguridad perimetral

2.1 UNICAN:

Se suministrará un sistema de seguridad perimetral formado por al menos 2 equipos situados uno en cada uno de los CPD's y con capacidad de funcionamiento activo/activo, con todos los elementos que forman cada equipo redundados y "espejado" en el CPD equivalente. Deberá contar con sistemas de detección de intrusión (IPS), denegación de servicios (DoS), NAT y calidad de servicio (QoS), todo ello funcionando a pleno rendimiento, bajo diferentes tipos de enlaces, redes y el mismo sistema operativo. Los equipos que formen parte del sistema deben ser idénticos en todos los aspectos: técnicos, enlaces, funcionalidades,…. Las características técnicas mínimas exigidas son:

- Número de usuarios soportado ilimitado
- Capacidad de ampliación, crecimiento y expansión en cuanto a tarjetas.
- Soporte para interfaces del tipo: Ethernet 10/100/1000 en cobre, Gigabit Ethernet y 10 Gigabit Ethernet en fibra en todas sus variantes, con módulos SFP, SFP+ y XFP
- Soporte de alta disponibilidad en modos: activo/pasivo y activo/activo con interfaces dedicados a dicha funcionalidad.
- Control de acceso seguro al equipo por todos los interfaces mediante el control de acceso (NAC)

definido en el proyecto.

- Capacidad de crear grupos de agregación de interfaces entre equipos formando parte del cluster.
- Filtrado y detección de:
    - Network attack detection.
    - DoS and DDoS protection.
    - TCP reassembly for fragmented packet protection.
    - Brute force attack mitigation.
    - SYN cookie protection.
    - Zone-based IP spoofing.
    - Malformed packet protection.
    - GPRS stateful inspection.
- Sistema de prevención de intrusión:
    - Active/active traffic monitoring
    - Attack detection mechanisms: Stateful signatures, protocol anomaly detection (zero-day coverage), application identification
    - Attack response mechanisms: Drop connection, close connection, session packet log, session summary, email, custom session
    - Attack notification mechanisms: Structured syslog
    - Worm protection.
    - Application Denial of Service protection.
    - SSL encrypted traffic inspection.
    - Simplified installation through recommended policies.
    - Trojan protection.
    - Spyware/adware/keylogger protection.
    - Other malware protection.
    - Protection against attack proliferation from infected systems.
    - Reconnaissance protection.
    - Request and response side attack protection.
    - Compound attacks — combines stateful signatures and protocol anomalies.
    - Create custom attack signatures.
    - Attack editing (port range, other).
    - Stream signatures.
    - Protocol thresholds.
    - Stateful protocol signatures.
    - Approximate number of attacks covered: mínimo 6.000
    - Detailed threat descriptions and remediation/patch info.
    - Create and enforce appropriate application-usage policies.

- Attacker and target audit trail and reporting.
- Deployment modes: Inline or TAP
- IPS monitoring on active/active chassis clusters.

- IPsec VPN
  - Site-to-site tunnels
  - Tunnel interfaces
  - DES (56-bit), 3DES (168-bit), and AES encryption
  - MD5 and SHA-1 authentication
  - Manual key, IKE, PKI (X.509)
  - Perfect forward secrecy (DH groups): 1,2,5
  - Prevent replay attack
  - Remote access VPN
  - Redundant VPN gateways
- Destination Network Address Translation
  - Destination NAT with PAT
  - Destination NAT within same subnet as ingress interface IP
  - Destination addresses and port numbers to one single address and a specific port number (M:1P)
  - Destination addresses to one single address (M:1)
  - Destination addresses to another range of addresses (M:M)
- Source Network Address Translation
  - Static Source NAT – IP-shifting DIP
  - Source NAT with PAT – port-translated
  - Source NAT without PAT – fix-port
  - Source NAT – IP address persistency
  - Source pool grouping
  - Source pool utilization alarm
  - Source IP outside of the interface subnet
  - Source Network Address Translation (continued)
  - Interface source NAT – interface DIP
  - Oversubscribed NAT pool with fallback to PAT when the address pool is exhausted
  - Symmetric NAT
  - Allocate multiple ranges in NAT pool
  - Proxy ARP for physical port
  - Source NAT with loopback grouping – DIP loopback grouping
- User Authentication and Access Control
  - Built-in (internal) database

- RADIUS accounting
- Web-based authentication
- NAC

- Public Key Infrastructure (PKI) Support
  - PKI certificate requests (PKCS 7 and PKCS 10)
  - Automated certificate enrollment (SCEP)
  - Certificate authorities supported
  - Self-signed certificates
- Virtualization
  - Security zones
  - Virtual routers
  - VLANs per interface
  - L3 subinterfaces
- Routing
  - BGP instances
  - BGP peers
  - BGP routes
  - OSPF instances
  - OSPF routes
  - RIP v1/v2 instances
  - RIP v2 table size
  - Dynamic routing
  - Static routes
  - Filter-based forwarding (FBF)
  - Equal-cost multipath (ECMP)
  - Reverse path forwarding (RPF)
- IP Address Assignment
  - Static
  - Dynamic Host Configuration Protocol (DHCP)
  - Internal DHCP server
  - DHCP relay
- Traffic Management QoS
  - Maximum bandwidth
  - RFC2474 IP DiffServ in IPv4
  - Filters for CoS
  - Classification
  - Scheduling

    - Shaping
    - Intelligent Drop Mechanisms (WRED)
    - Three-level scheduling
    - Weighted round-robin for each level of scheduling
    - Priority of routing protocols
- High Availability
    - Active/passive, active/active
    - Low impact chassis cluster upgrades
    - Configuration synchronization
    - Session synchronization for firewall and IPsec VPN
    - Session failover for routing change
    - Device failure detection
    - Link and upstream failure detection
    - Interface link aggregation
- Management
    - WebUI (HTTP and HTTPS)
    - Command-line interface (console)
    - Command-line interface (telnet)
    - Command-line interface (SSH)
- Administration
    - Local administrator database support
    - External administrator database support
    - Restricted administrative networks
    - Root admin, admin, and read-only user levels
    - Software upgrades
    - Configuration rollback
- Logging/Monitoring
    - Structured System Log
    - SNMP (v2/v3)
    - Traceroute
    - Power supply redundancy
- Certifications
    - Safety certifications
    - Electromagnetic compatibility (EMC) certifications
- Administración basada en roles.
- Programación de actualizaciones de seguridad,
- Gestión por dominios, con separación lógica de dispositivos, políticas, reportes,…

- Bloqueo de objetos para evitar cambios accidentales de configuraciones.
- Programación de copias de seguridad de la configuración.
- El equipo dispondrá del número de interfaces necesarios requeridos en el pliego para el correcto funcionamiento activo/activo y única unidad lógica, según los gráficos.

2.2 Aulas/Salas

Se suministrará un segundo sistema de defensa perimetral, con las mismas funcionalidades y servicios que el detallado anteriormente, que se encargará de la seguridad de todo el sistema de aulas y salas que dispone actualmente la Universidad de Cantabria. Dispondrá al menos de 4 enlaces de 10Gb.

2.3 VPN-SSL

La Universidad de Cantabria, dispone actualmente de un equipo Juniper SA4500 para el acceso tanto remoto, como por WiFi para toda su comunidad universitaria, a través del protocolo VPN-SSL. Se suministrará para completar el actual sistema de acceso remoto, mediante VPN-SSL, un equipo similar al actual Juniper IVE 4500, con licencia para al menos 750 usuarios simultáneos y con todas las licencias y aplicaciones necesarios para operar en alta disponibilidad. El ofertante podrá reemplazar dicho sistema por otro fabricante, siempre y cuando cumpla las mismas condiciones actuales de funcionamiento y las señaladas anteriormente, deberá indicarlo en su oferta. En caso de sustituir el sistema deberá detallar el modelo y características en la documentación adicional solicitada en el Anexo I.

2.4 Gestor de Ancho de Banda.

La Universidad de Cantabria, dispone actualmente de un equipo Allot NetEnforcer AC-804 con un caudal gestionable de 155Mb/s full-duplex junto con la aplicación Allot NetXplorer - Bandwidth Reporting and Monitoring instalada en un servidor, para la gestión y control de la conexión a Internet. Se deberá suministrar un aumento de la capacidad del caudal gestionable a 310 Mb/s full-duplex. El ofertante podrá reemplazar dicho sistema por un Allot NetEnforcer 1440 o similar, con las mismas características técnicas y funcionalidades requeridas. Así mismo se suministrará el servidor y aplicación que se encargue de gestionar, monitorizar, reportar y contabilizar el tráfico que circula por el dispositivo. En caso de sustituir el sistema deberá detallar el modelo y características en la documentación adicional solicitada en el Anexo I.

3.- Plataforma de Gestión

3.1 Gestión de red

Dentro de la arquitectura de gestión de la red, se requiere la oferta de un sistema de Gestión de la Información de Seguridad (Security Integrated Manager) que permite recoger toda la información proveniente de múltiples fuentes en una sola consola para consolidar, correlar, normalizar y priorizar la información de qué sucede dentro de la red, mejorando en gran medida la capacidad de una organización de responder a cualquier problema de seguridad que surja.

Su disposición en forma de cuadro de mandos configurable por el gestor debe permitir además recoger de forma sencilla la información de seguridad más relevante.

El sistema deberá incluir soporte todo tipo de productos de múltiples fabricantes, y la posibilidad de añadir módulos para el soporte de cualquier otro sistema o aplicación que pueda ser necesario. Soporta de forma nativa múltiples productos como firewalls, IDS/IPS, antivirus, balanceadores de carga, VPN's SSL, herramientas de análisis de vulnerabilidades, y otros.

El formato será el de un appliance que recoge toda la información de las diversas fuentes, y de otros appliances de segundo nivel, que hacen las veces de sondas de red, para analizar el tráfico y construir estadísticas de uso de aplicaciones en diferentes zonas de la red. Estos appliances de segundo nivel proporcionarán además la capacidad de actuar como sondas IDS en lo que se refiere al análisis de flujos anormales de tráfico, completando las posibilidades que ofrecen las tecnologías de Pattern Matching y de Análisis de Protocolos.

Las funcionalidades requeridas del sistema de información sobre la gestión de sucesos de seguridad SIEM (Security Information Event Management and log managament) son las siguientes:

- Integrar todos los elementos de seguridad en la red en una única consola de control y cuadro de mandos que es capaz de recoger, correlar, normalizar y priorizar toda la información, y mejorar así la capacidad de la organización para responder a los eventos de seguridad que puedan surgir
- Aprovechar la información de todos los equipos de red y de seguridad para proporcionar una visibilidad total y un control mejorado de las comunicaciones
- Reducir la sobrecarga de eventos de seguridad de la red a una lista manejable y que establece las prioridades de trabajo
- Proporcionar informes de seguridad y de cumplimiento para comprobar el alineamiento de la seguridad con los objetivos de la organización
- Priorizar la información de comportamientos maliciosos y presentar los pasos prácticos a seguir para su resolución
- Interoperabilidad total con dispositivos de otros fabricantes y con herramientas de resolución avanzada del sistema de gestión de red, para una respuesta dinámica
- Soporte de fuentes de flujos, netflow, jflow, sflow, packeteer, etc.
- Soporte de un mínimo de 5.000 eventos por segundo y 200.000 flujos bidireccionales.
- El coste de la plataforma debe ser independiente de la cantidad de nodos monitorizados.

Los appliances del SIEM dispondrán de interfaces Gb Ethernet 10/100/1000 y 1000Base-SX para su conexión a la red.

Se situarán en el interior de los CPD's para analizar los flujos de tráfico que se establecen hacia los servidores, pero tendrá la posibilidad de colocarse en cualquier otro punto de la red. El dimensionamiento

del sistema se hará en base a la capacidad de los enlaces y sistemas de los que recoge los flujos de tráfico a inspeccionar y de los eventos a recibir.

La configuración y gestión de esta plataforma se realiza a través de un interfaz web seguro, que será además la encargada de mostrar la información recogida de todos los demás sistemas en una única consola de control de la red.

La plataforma SIM se conectará a la red de forma pasiva, en puertos destinados a la monitorización mediante la configuración de funcionalidades de port mirroring o mediante el uso de network taps.

Así pues, no deberá constituir un punto de fallo. En cualquier caso, se redundarán todos los appliances del sistema, tanto sondas como servidores. La gestión debe realizarse mediante un interfaz web seguro desde cualquier estación de la red.

El sistema de disco de los appliances será RAID 5 para mayor fiabilidad de la plataforma hardware.

La gestión de la red es un aspecto que toma cada día más relevancia. La dimensión y criticidad de una red como la de la Universidad de Cantabria precisa de una plataforma de gestión capaz de monitorizar el estado de toda la red, obtener estadísticas relevantes para la monitorización del rendimiento de equipamiento y aplicaciones críticas, y sobre todo simplificar tareas complejas en un entorno geográficamente extenso.

La plataforma software de gestión ofertada ofrecerá unas capacidades de monitorización de la red a medida, integrando en una sola aplicación la gestión de múltiples dispositivos y fabricantes. Facilitará tareas como:

- El descubrimiento automático y organización lógica y automatizada de dispositivos en grupos según diferentes criterios: localización, tipo de dispositivo, persona encargada de su gestión, direccionamiento IP, o por cualquier otro criterio que se desee utilizar.
- La organización lógica de grupos de puertos según la topología de la red y sus funciones: puertos de usuario, de enlace, de servidores,… o por cualquier otro criterio que se desee utilizar.
- La localización de direcciones MAC, direcciones IP, máquinas y usuarios dentro del entorno de red deseado, de forma automática y en pocos segundos.
- El despliegue de VLANs mediante la creación de modelos, de forma rápida y sencilla que permita descargar una plantilla común de VLANs a múltiples dispositivos, o verificar y modificar la configuración de múltiples puertos con una sola acción.
- La creación automática de mapas en base a aspectos topológicos a diferentes niveles: conexiones físicas, topologías de Spanning Tree, topologías de nivel 3, distribución de VLANs,…
- La monitorización automatizada de múltiples parámetros de funcionamiento de cualquier

dispositivo mediante el uso de plantillas predefinidas y personalizables por el usuario, así como la exportación de la información a formatos web, Excel y de texto, para el uso de cualquier usuario que quiera consultarla en diferentes formatos.

- La consolidación y gestión de alarmas, syslog, traps y eventos en un único visor para la totalidad de dispositivos de la red, así como la posibilidad de ejecutar procesos de forma automatizada ante diferentes alarmas y eventos que se puedan producir.

- El despliegue de políticas de seguridad, personalización y priorización de tráfico de forma estática o dinámica dentro de toda la red, de forma rápida y sencilla.

- La capacidad de localización de sistemas fuente de problemas dentro de la red, y de respuesta activa y automatizada frente a dichos problemas, de forma integrada con otros elementos de seguridad, como cortafuegos, antivirus e IDS's.

- Debe ser capaz de documentar de manera eficiente y actualizar los datos de la red en constante cambio. Simplificando el despliegue y la gestión de los dispositivos de red. Que permita realizar fácilmente una amplia lista de tareas de gestión como son: la administración de los archivos de configuración de los dispositivo, copias de seguridad, actualizaciones de firmware, datos de archivo de configuración, o restaurar uno o varios dispositivos, Schedule. Capaz de identificar los puertos no utilizados y las ranuras del chasis/stack, altas y cambio. Inventariado la red, rastreando cambios de configuración para los dispositivos de red.

Todo esto basado en una arquitectura centralizada cliente/servidor. La aplicación hará uso de una serie de servicios que usen una base de datos única y gestiona el acceso a la misma de usuarios remotos, de forma que varios usuarios pueden conectarse al servidor de manera simultánea, y realizar las tareas que precisan.

Estos usuarios remotos harán uso de clientes ligeros y sin coste, y simultáneamente podrán acceder al servidor, en las mismas condiciones que se dan en la consola central, un máximo de 25 clientes, aunque el número de clientes que se pueden instalar no tiene ninguna limitación. Mediante la autenticación en el dominio, cada uno de ellos accede a los servicios del servidor con un nivel de acceso personalizado para restringir las tareas al alcance de cada uno de ellos. De esta forma, un usuario podrá añadir o eliminar dispositivos de la base de datos siempre que su perfil se lo permitiera, mientras que otro no tendrá esa capacidad y sólo le sería dado acceso a la base de datos para monitorizar el comportamiento de los equipos y visualizar las alarmas.

La plataforma de gestión estará abierta a la configuración, gestión y monitorización de cualquier elemento gestionable por SNMP en cualquiera de sus versiones (v1/v2c/v3).

Además, debe permitir la consolidación de todo tipo de notificaciones (traps e informes SNMP, eventos, mensajes de syslog en diferentes formatos…) sobre la propia aplicación. Toda esta información se almacena en una base de datos para su posterior procesamiento y análisis.

Asimismo, se pueden enviar notificaciones de todo tipo desde la propia aplicación en función de la

información recogida, así como ejecutar aplicaciones externas con multitud de parámetros y argumentos.

El sistema será capaz de almacenar, al menos los logs recibidos de toda la infraestructura de red por un periodo mínimo de 2 años, siendo recuperable la información de forma sencilla e intuitiva. También se incluirán todas aquellas licencias que fueran necesarias para utilizar todas funcionalidades requeridas.

3.2 Sistema de control de accesos (NAC)

El sistema NAC (Network Access Control/Control de Acceso a Red), deberá estar basado en el estándar TNC (Trusted Network Connect) que engloba a la práctica totalidad de fabricantes de hardware, software y seguridad denominado TCG (Trusted Computing Group).

El objetivo consiste en ser capaz de evaluar el estado de un sistema final en lo referente a su seguridad, para tomar una decisión en cuanto a si dicho sistema debe ser autorizado a entrar en la red o no. Esta evaluación puede realizarla un agente instalado en el propio sistema, o un sistema externo a través de herramientas tipo Nessus o Lockdown. También deben tomarse en consideración otros aspectos como la franja horaria en la que tiene lugar el intento de acceso a la red, la localización física del sistema, y otros.

El resultado positivo de dicha evaluación permitirá al sistema final completar con éxito el proceso de autenticación en la red. Si de la evaluación resulta que el sistema no cumple con la política de seguridad corporativa, debe ser la infraestructura de comunicaciones la que proporcione el mecanismo de contención para dicho sistema, pasando a permanecer en un estado de cuarentena.

En resumen, el sistema NAC cumplirá:

Autenticación – Controlar a quién se permite el acceso. Esto es generalmente realizado para obligar al usuario a autenticarse antes de que se le conceda acceso a la red. Esta autenticación puede ser en forma de un nombre de usuario y contraseña, una dirección MAC única, o un sistema de huellas dactilares, DNI,….

Evaluación - Determinar si el cliente cumple con los requisitos de seguridad antes de permitir que entre en la red. El objetivo final es reducir el riesgo a exponerse a un equipo no seguro revisando la seguridad del ordenador. Por lo general, esto implica asegurarse de que el ordenador tiene actualizado los parches de seguridad del sistema operativo, el software anti-virus(AV), anti-spyware software(AS), y no está activamente infectado con un virus o gusano. También es deseable una evaluación continua y permanente.

Cuarentena y Remediación - Cualquier cliente que no cumpla los requisitos de seguridad, debe ponerse en cuarentena y ofrecerle medidas de remediación. Mientras en la red de cuarentena, le permite acceso a la red, limitado sólo a los recursos de rehabilitación que son necesarias para que cumpla los requerimientos de seguridad. La rehabilitación la llevará a cabo el usuario final, el proceso debe ser intuitivo y poco exigente. Cuanto más automatizado mejor.

Autorización - Controlar el tipo de acceso a la red del cliente. El objetivo final es limitar el acceso a la red, tanto como sea práctico, sólo a aquellos recursos que el usuario realmente necesita. El tipo de acceso a la red es, normalmente, en base a la identidad del usuario y la normativa de seguridad de la empresa.

Automatizado revisión / actualización de versión – El sistema debe ser capaz de actualizar regularmente sus

controles de seguridad. Como mínimo, los controles de seguridad que se ocupan de la inspección de la actualización de AV, AS y la seguridad del sistema operativo deben ser automáticos. Si la actualización de estos controles se auto-cumple y depende de su entorno, pero la opción debe estar disponible. El propósito de utilizar la función automática de actualización de la seguridad es para eliminar la pesada carga de tener que realizarlo a mano, realizando un seguimiento de las actualizaciones publicadas por los proveedores y para qué versión de su producto. A continuación, la traslación de toda esa información en un control de seguridad, que hará una inspección correctamente.

Gestión Centralizada – El sistema NAC debe ser manejable y con gestión centralizada. Normalmente, un gran sistema NAC incluirá varios componentes individuales. Idealmente, un sistema centralizado de gestión debe ser capaz de gestionar todos los componentes individuales. Las características de la gestión centralizada son:

1. Control de acceso y contabilidad
2. Incremento de la coherencia y la precisión de las configuraciones a través de múltiples componentes NAC
3. Simplifica la gestión de la política de múltiples componentes NAC.
4. Seguimiento centralizado del usuario, presentación de informes y auditoría

Colaboración – Un sistema NAC debe poder interoperar con otras redes, con la seguridad y la autenticación de dispositivos. Como mínimo, debe ser capaz de trabajar con LDAP existente, AD, y los servidores de autenticación RADIUS para la autenticación de usuarios. Debe ser capaz de interoperar con conmutadores de LAN existente para la VLAN basada en puerto de conmutación. Y por último, debe interoperar con Microsoft para la gestión de parches y con los más destacados AV y mantenerlos actualizados.

Adaptable – El sistema NAC debe estar aplicado en toda la red interna para que sean más eficaces. Todos los clientes tratando de acceder, por cualquier medio, a los recursos de la red interna debe ser autenticado, evaluado y autorizado. Los puntos comunes de entrada incluyen: cable, conexión inalámbrica, VPN, WAN,... La robustez de todos los puntos de entrada en la red interna de esta manera, dará el control último sobre quién, cómo, cuándo, dónde, se conecta con sus recursos internos.

Alta disponibilidad - Todos los componentes críticos del sistema NAC deben ser redundados y tolerante a fallos. En caso de fallo completo del sistema NAC, no debe permitir el acceso de nadie.

Las funcionalidades de éste sistema no se limitarán a la gama de soluciones NAC, sino que tendrá aplicación en muchos otros apartados, como puede ser el servir de herramienta de registro de MAC's, histórico de intentos de acceso y de movimientos dentro de la red, o como herramienta para el soporte de entornos de virtualización de servicios en CPD's. En esta última situación se muestra la flexibilidad de la arquitectura de red, que apoyándose en la plataforma NAC mejora el control y el nivel de seguridad de este tipo de soluciones, aspectos que son difíciles de manejar toda vez que la virtualización permite migrar físicamente un servicio de un punto del CPD a otro, complicando la gestión manual de la infraestructura de

comunicaciones.

Las funcionalidades que aporta el sistema NAC deberán ser las siguientes:

- Definición y configuración de dominios de seguridad dentro de la red.
- Registro automático de direcciones MAC en la red.
- Registro histórico de intentos de conexión a la red y localizaciones físicas.
- Control de acceso en función de los puertos físicos desde donde se intenta acceder a la red.
- Control de acceso en función de la franja horaria y día de la semana en que se intenta acceder a la red.
- Control de acceso en base a la creación de listas blancas y negras de usuarios y sistemas.
- Soporte de entornos de virtualización de aplicaciones en los CPD's, para dotarlos de mayor control y seguridad automatizados.
- Seguridad proactiva mediante el análisis de vulnerabilidades de los sistema finales.
- Monitorización y reporte del estado de los sistemas conectados a la red.
- Integración con múltiples fabricantes.
- Soporte de sistemas de evaluación(assessment) externos o integrados en la plataforma.
- Soporte de funciones de evaluación desde la red para cualquier sistema operativo.
- Soporte de clientes específicos para evaluación(assessment).

El formato será el de appliances o módulos integrados en los equipos de red. Los appliances dispondrán de interfaces Gb Ethernet en 10/100/1000 y 1000Base-SX para su conexión a la red. Se sitúan en el entorno de los CPD's, ya que tienen una fuerte relación con los servidores Radius para la gestión de la identidad y control de acceso a la red.

Se integrará con cualquier electrónica que soporte el estándar de autenticación 802.1x con capacidad para asignar VLANs dinámicamente (RFC3580). Se integra también con cualquier servidor Radius estándar del mercado, así como con herramientas de análisis de vulnerabilidades como Nessus, y con soluciones basadas en agentes como las de Microsoft NAP, Symantec, Checkpoint y muchas otras.

La configuración y gestión de estos appliances se realizan desde la aplicación de gestión como parte de una arquitectura de gestión unificada con la red.

La redundancia del sistema NAC contemplará a todos los elementos del propio sistema. Se redundarán los

appliances que centralizan las peticiones de autenticación para el acceso a la red, la gestión de los mismos en la aplicación de gestión, los servidores Radius para la gestión de la identidad, y las herramientas de análisis de vulnerabilidades definidas en el sistema.

En caso de no poder establecer comunicación bien con los servidores Radius, bien con las herramientas de análisis de vulnerabilidades definidas, puede optarse por facilitar el acceso de los sistemas a la red mediante la asignación de una política definida expresamente para este caso.

4.- Instalación y Configuración

Para la fase de instalación y configuración del suministro, se designará por parte de la empresa adjudicataria, un equipo de trabajo, formado por las siguientes tipos de profesionales:

- Director: Analista de comunicaciones con 5 años de experiencia en instalaciones similares, con el mismo tiempo en la empresa adjudicataria y con las máximas certificaciones del fabricante de los diferentes productos ofertados.
- 2 analistas de comunicaciones: con 3 años de experiencia en instalaciones similares , con el mismo tiempo en la empresa adjudicataria y con las máximas certificaciones del fabricante de los diferentes productos ofertados.
- 4 técnicos de comunicaciones: con 2 años de experiencia en instalaciones similares y mismo tiempo en la empresa adjudicataria.

Deberá acreditarse la documentación profesional y experiencia requerida en el párrafo anterior. El equipo de trabajo deberá estar operativo y disponible a cualquier hora del día y de la semana para realizar las diferentes operaciones de los procesos de instalación y configuración, en horas que afecten lo menos posible al sistema actualmente en funcionamiento, durante el periodo que se oferte hasta la finalización del procedimiento, ya que al tratarse de sustituir equipamiento de una red en producción, habrá que realizar los cortes pertinentes en los momentos que menos se perjudique a los usuarios de la red UNICAN.

Se instalarán y configurarán los equipos según los parámetros que defina el Servicio de Informática de la Universidad de Cantabria. Así mismo los equipos quedarán instalados en los rack´s de comunicaciones y se realizará el conexionado de todas las tomas de usuario que existan en cada armario a los puertos de los equipos suministrados; además se suministrarán los latiguillos de cobre, CAT 5e y de fibra óptica en el tipo correspondiente, correctamente etiquetados. Se entregará toda la documentación de asignación de puertos y tomas en una hoja tipo Excel. Todo el pequeño material (tuercas, tornillos, bridas,…) necesario para una correcta instalación en los racks's será suministrado por el licitador.

Para todo el material suministrado, si hubiera prestaciones que requieran de software , licencias, hardware adicional, etc. deberá incluirse en la oferta.

Todo el material objeto del suministro que se oferte no debe encontrarse incluido en procesos de discontinuidad, descatalogación o fin de vida del fabricante. Además, el suministrador deberá garantizar la vigencia del material, como mínimo, durante los 4 años siguientes a la formalización del contrato. Para

garantizar éste aspecto, la Universidad de Cantabria podrá solicitar al fabricante del producto ofertado el "roadmap" de dicho producto, durante el proceso de adjudicación.

Todas las funcionalidades requeridas deben poder implementarse o configurarse simultáneamente, sin que afecte al rendimiento del equipo y sus prestaciones no se degraden.

Se exige, que las funcionalidades requeridas se soporten siguiendo los estándares internacionales frente a implementaciones propietarias.

El equipamiento propuesto debe estar avalado por una experiencia de operación en un entorno en producción, de al menos 6 meses.

5.-Garantía

El suministro tendrá una garantía de 4 años, directamente contratada con los fabricantes y extendida a favor de la Universidad de Cantabria para todo el material suministrado (hardware, software, licencias,…,)

La garantía por 4 años constará de las siguientes características mínimas:

- HELP DESK
    - Gestión y atención de Incidencias
    - Gestión de Reemplazos
    - Gestión de Stock
    - Gestión de Garantía.
    - Informe accesible vía web de incidencias.
    - Atención a consultas del servicio.
- Apertura de casos con el fabricante y gestión de garantía extendida incluida.
- Mantenimiento correctivo
    - Primer nivel (reemplazo y resolución in situ).
    - Segundo nivel (conocimiento avanzado, diagnóstico remoto y resolución).
    - Tercer nivel (conocimiento experto, escalado a fabricante).
- Gestión del software
    - Suministro de información de nuevas actualizaciones.
    - Actualizaciones correctivas.

- Acuerdo de Nivel de Servicio (SLA): 8x5xNBD (Next Bussiness Day)
    - Se considera “tiempo de respuesta”, como el tiempo desde que el personal de la Universidad de Cantabria se pone en contacto con el equipo de soporte del licitador para escalar una incidencia hasta que una persona de la empresa licitadora contacta con el personal del cliente para comenzar el estudio y solución del problema.

- Soporte técnico en España y en castellano.

6.- Formación

Se deberán suministrar cursos de formación en las instalaciones de la Universidad de Cantabria, para al menos 5 personas de la propia universidad de todo el equipamiento, prestaciones y funcionalidades suministradas, debiéndose detallar el contenido y duración de cada uno de ellos. Toda la formación, deberá ser la oficial y certificada por el fabricante del producto y con personal docente certificado por el mismo fabricante. Los cursos permitirán conocer, instalar, configurar, mantener y resolver problemas de todo el material objeto de suministro. Si alguno de los cursos, conlleva la certificación del personal de la Universidad de Cantabria en los productos del fabricante, la oferta incluirá el pago de dichos derechos de certificación para cada uno de los alumnos.

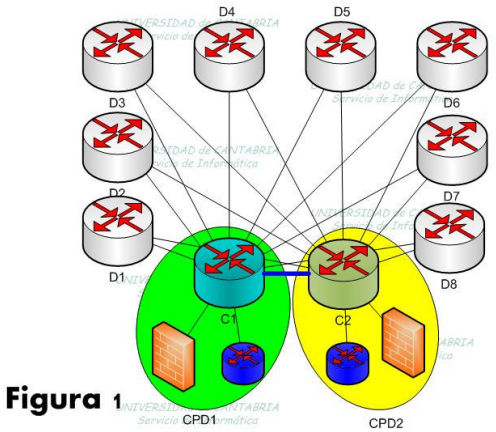

Figura 1

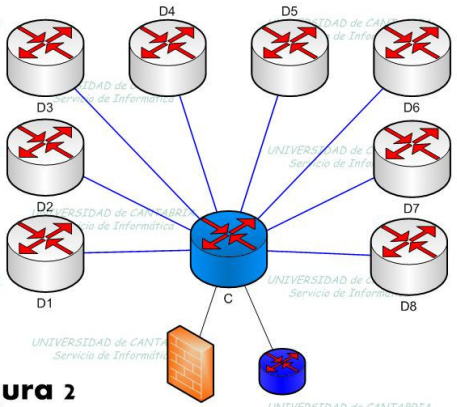

Figura 2

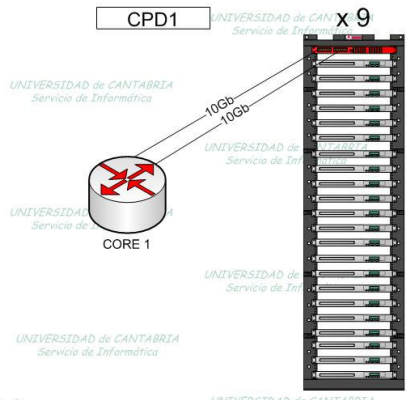

Figura 3

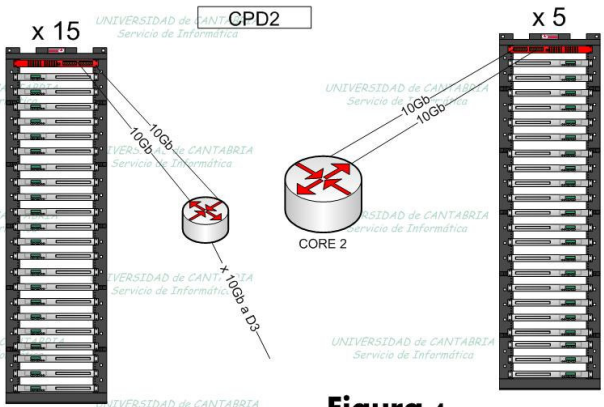

Figura 4

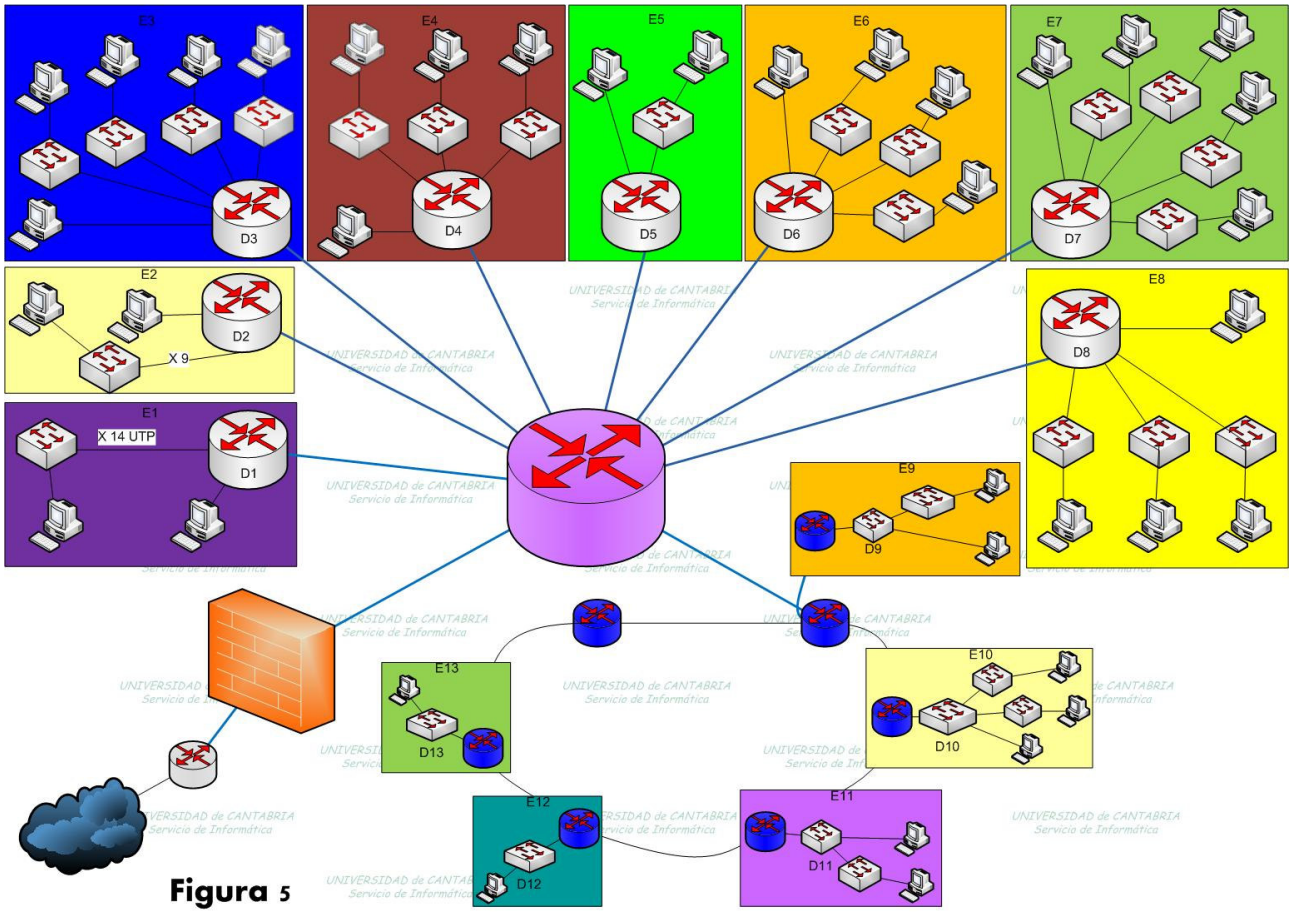
E3
D3
E4
D4
E5
D5
E6
D6
E7
D7
E2
D2
X 9
E8
D8
E1
X 14 UTP
D1
E9
D9
E13
D13
E10
D10
E12
D12
E11
D11

Figura 5

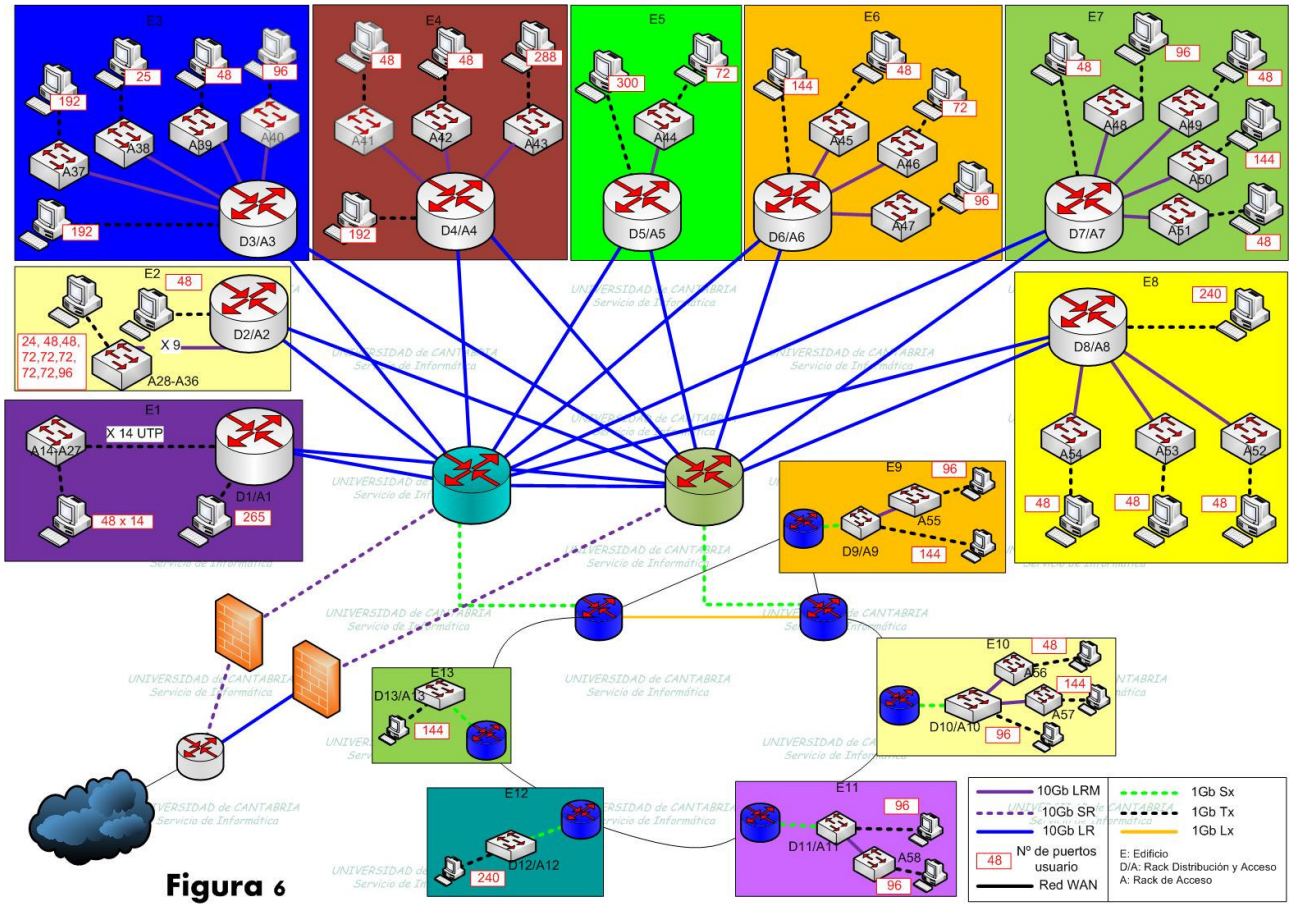

Figura 6

PRESUPUESTO BASE DE LICITACIÓN, IVA INCLUIDO: 1.125.000,00.-€