UNIVERSIDAD DE BURGOS | Servicio de Informática y Comunicaciones

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA ADQUISICIÓN Y MANTENIMIENTO DE EQUIPAMIENTO DE SEGURIDAD PERIMETRAL PARA LA UNIVERSIDAD DE BURGOS

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

1. OBJETO

El objeto del presente procedimiento es la adquisición, implantación, configuración, soporte y mantenimiento de una solución de seguridad perimetral basada en firewalls de nueva generación, destinada a sustituir los sistemas actualmente en producción, con el fin de adaptarse al crecimiento de las necesidades de la red y garantizar un nivel adecuado de seguridad en las infraestructuras de la Universidad de Burgos (UBU).

La solución deberá permitir incrementar la capacidad de ancho de banda, pasando de los 10Gb actuales a 100Gb, asegurando el rendimiento necesario para el tratamiento del tráfico de red presente y futuro, así como la correcta aplicación de las políticas de seguridad.

El contrato incluye la prestación de los servicios necesarios para la correcta puesta en funcionamiento de la solución, tales como:

- Instalación y configuración del equipamiento.
- Migración de la configuración y de las políticas de seguridad existentes.
- Formación técnica.

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

- Servicios de soporte y mantenimiento.

Además, se debe garantizar la continuidad del servicio y la mínima afectación al mismo realizando la implantación en los plazos indicados en **el apartado 5 de este pliego técnico.**

La empresa adjudicataria se comprometerá a atender y resolver las incidencias comunicadas por la Universidad de Burgos, derivadas de averías, cambios de configuración programados, actualizaciones de versiones y mantenimiento preventivo y correctivo de los equipos objeto del contrato.

Este pliego de prescripciones técnicas recoge las condiciones mínimas que debe cumplir la oferta presentada y que se detallan a continuación.

2. SITUACIÓN ACTUAL

Actualmente la Universidad de Burgos cuenta con dos equipos **Palo Alto modelo PA 5220**, en alta disponibilidad en configuración activo-pasivo, con las siguientes licencias y subscripciones:

a. Threat Prevention
b. Advanced Threat Prevention
c. WildFire License (WildFire signature feed, integrated WildFire logs, WildFire API)
d. Advanced WildFire (signatures, logs, API)
e. GlobalProtect Gateway License
f. DNS Security Subscription
g. Advanced DNS Security Subscription
h. Palo Alto Networks URL Filtering License
i. Advanced URL Filtering
j. SD WAN License
k. Advanced SD WAN License
l. Premium Partner Support

3. REQUISITOS DEL SUMINISTRO

Se requiere el suministro de dos sistemas NGFW (Next Generation Firewall) físicos idénticos, modelo **Palo Alto PA-3430 Hardware Appliance** o equivalente, para su instalación en alta disponibilidad, permitiendo tanto modo activo-activo como activo-pasivo. La arquitectura deberá garantizar la continuidad del servicio ante fallos, de forma transparente para los usuarios.

El equipamiento a suministrar integrará las redes, políticas de filtrado y conexiones

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

VPN existentes actualmente, manteniendo y ampliando, en su caso, todas las funcionalidades actuales indicadas en el **apartado 2**. Si

Por tratarse de equipos en producción, que forman parte de la seguridad perimetral de la red corporativa de la Universidad, se requiere que los equipos sean del mismo fabricante actual para garantizar una fácil integración con el resto de la infraestructura de seguridad existente. El esfuerzo de migración e integración que se debería realizar implantando una solución de otro fabricante condiciona de forma determinante el tiempo de implantación y podría suponer un cambio tecnológico que incremente el riesgo de indisponibilidad y/o la duración del despliegue en un sistema crítico como es la seguridad de la red corporativa.

Se requiere que todos los componentes, hardware y software, necesarios para el correcto funcionamiento del equipamiento objeto del suministro tengan una permanencia mínima **de 6 años desde la firma del contrato** y, consecuentemente, no se encuentren incluidos en procesos de discontinuidad, descatalogación o fin de vida del fabricante. **Los licitadores deberán incluir en sus propuestas un documento del fabricante certificando dicha situación.**
Si por circunstancias excepcionales se produjera la descatalogación de algún producto software incluido en este contrato durante el mencionado plazo de 6 años, la empresa adjudicataria estará obligada a proveer a la universidad de la nueva versión sustitutiva sin coste adicional, siendo también por su cuenta la migración de los correspondientes servicios a la nueva versión.

Se deberá garantizar la existencia de repuestos durante todos los años de duración del contrato (incluidas las posibles prórrogas).

La oferta incluirá todos aquellos componentes, materiales, elementos de conexión (fibras, SPF+, cables, latiguillos, etc.), licencias, mano de obra, desplazamientos y otros gastos relacionados con la ejecución del contrato, durante toda la duración del mismo incluidas las posibles prórrogas.

La Universidad requiere que todos los equipos y software objeto del contrato estén respaldados mediante contratos de soporte en vigor en 24*7, con los fabricantes durante toda la duración del contrato incluidas las prórrogas.

3.1. REQUISITOS GENERALES

A continuación, se detallan las características hardware que debe cumplir **cada uno de los dos equipos** objeto de la licitación.

1. El equipo debe estar incluido en el Catálogo de Productos y Servicios de las Tecnologías de la Información y la Comunicación (CPSTIC)CPSTIC del CCN.

2. Debe contar con una guía de seguridad del CCN.

3. Debe ser capaz de manejar como mínimo 150.000 nuevas sesiones por segundo.

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

4. Poder crear, al menos, 10 cortafuegos virtuales (incluidas las licencias).

5. Número mínimo de sesiones SSL descifradas concurrentemente: 250.000.

6. Capacidad del firewall con la identificación de aplicaciones habilitada (es decir, trabajando a nivel 7 para todo el tráfico): 18 Gbps.

7. Capacidad con todos los servicios de seguridad habilitados, incluyendo todas las subscripciones indicadas en el apartado 2, tanto a nivel de prevención frente a amenazas conocidas (IPS, Antivirus, Antispyware, URL Filtering, etc.) como frente a amenazas desconocidas (Sandboxing): 9 Gbps.

8. Visualización de número de usos y cantidad de tráfico de cada regla, así como de la última vez que se ha utilizado.

9. Funcionalidad integrada de Traffic Shaping tanto de tráfico saliente como entrante, siendo capaz de reservar ancho de banda y marcar el tráfico con DSCP.

    a. Deberá permitir la creación de firmas específicas de IPS.
    b. Deberá permitir el control de la navegación por categorías de URL, así como trabajar con listas blancas y negras.

10. Deberá disponer como mínimo de:

    a. Al menos 8 interfaces 10GE SFP+ (con sus respectivos SFP+).
    b. Al menos 2 interfaces 40G/100G con 2 QSFP28 100G por cada equipo.
    c. 1 puerto de tipo DAC (dedicado a la gestión fuera de banda).
    d. Puerto de consola.
    e. Puertos dedicados a funciones propias del HA (sincronización de configuración, de sesiones, etc.) sin necesidad de utilizar puertos de servicio para esta tarea.
    f. Al menos 4 puertos 10/100/1000/10G RJ45.
    g. Doble fuente de alimentación redundada Hot-swap.
    h. Almacenamiento SSD (Solid State Disk) para almacenar sistema y configuración.

11. No debe superar 3U de montaje en rack.

12. Debe tener fuentes de alimentación y ventiladores redundantes.

13. Con el fin de cumplir con los objetivos de sostenibilidad y eficiencia energética, el consumo eléctrico máximo del equipo a plena carga no deberá superar los 250 W.

3.2. RENDIMIENTO

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

14. Se ha de garantizar que el firewall ofertado, no sufrirá degradación conforme se vayan habilitando perfiles de seguridad relacionados con la protección, es decir tanto a nivel de prevención frente a amenazas conocidas (IPS, Antivirus, Antispyware, URL Filtering, etc.) como frente a amenazas desconocidas (Sandboxing), de forma que sea predecible el impacto en el rendimiento de la solución en la activación progresiva de estas funciones de seguridad, independientemente del número de ellas.

15. La arquitectura hardware habrá de proveer procesadores específicos para el descifrado de tráfico.

16. No deberá haber mayor impacto por el hecho de habilitar más o menos firmas en los servicios de inspección de amenazas conocidas (IPS, Antivirus, Antispyware, URL Filtering, etc.).

17. Recursos hardware dedicados e independientes para el plano de control y para el de servicio, con el objetivo de poder garantizar que una sobrecarga del hardware destinado a prestar el servicio, no afectará a la gestión y viceversa.

18. La arquitectura hardware de la plataforma deberá permitir la aplicación paralela de diferentes módulos de seguridad, asegurando una sola inspección por cada paquete.

3.3. CARACTERISTICAS DE RED BÁSICAS

Cada firewall ofertado deberá tener las siguientes características técnicas de red básicas, entendiéndose como funcionalidades mínimas a cumplir:

19. Soporte de protocolos RIP v2, OSPF, BGP y Multicast para IPv4 e IPv6.
20. Routing basado en política.
21. Capacidad de realizar policy base routing en base a IP o red de origen, o también basado en usuarios/grupos o por tipo de aplicación.
22. Soporte Dual Stack IPv4 e IPv6 simultáneamente.
23. Network address translation NAT IPv4, NAT64.
24. DHCP server / DHCP Relay.
25. Soporte de DHCP, NAT y PAT.
26. NTP Server opcional.
27. Soporte de IEEE 802.1Q y agregación de interfaces mediante 802.1AD soportando hasta 8 grupos de agregación con 8 interfaces cada grupo.
28. Capacidades de virtualización: el cortafuegos debe poder virtualizarse en dominios que funcionen como cortafuegos independientes a los que se pueden aplicar diferentes configuraciones.
29. Capacidad de crear enlaces LACP para la agregación de puertos (802.3ad).
30. Capacidad de soportar arquitecturas de alta disponibilidad de tipo activo/pasivo o activo/activo.

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

3.4. VISIBILIDAD Y PROCESAMIENTO DE LOGS

Respecto a los logs se deberán cumplir las siguientes características:

31. Se enviarán los logs completos a una plataforma de gestión y procesamiento especializada (instalada on-premises) con objeto de mantener dichos logs a largo plazo sin pérdida de información, durante un **periodo mínimo de 1 año**.

32. Se deberá disponer de un cuadro de mando personalizable para cada usuario que acceda al sistema con al menos la siguiente información: aplicaciones más usadas, aplicaciones de alto riesgo, información general del sistema, estado de los interfaces, logs relativos a las amenazas más observadas, logs de filtrados URL o recursos del sistema, usuarios que más generan tráfico, las reglas de seguridad que más se usan, vulnerabilidades que más se han detectado y bloqueado, equipos que navegan hacia dominios maliciosos, virus detectados, e información enviada a los servicios de sandboxing o host comprometidos en la red interna.

33. Capacidad de uso de motor integrado de correlación de eventos dentro de la propia plataforma de forma que a partir de los logs recibidos se pueda obtener información como un listado de equipos comprometidos en la red interna y las evidencias que han dado lugar a dicho listado, con indicación de tiempos, usuarios, direcciones IP y vulnerabilidades o amenazas detectadas.

34. Posibilidad de filtrar cada una de las vistas o cuadros de mando de forma que la información esté restringida a ciertos criterios para poder realizar análisis más exhaustivos.

35. Funcionalidad de visualización de logs con diferentes niveles de agrupación (origen, destino, aplicación, amenaza, websites, etc.) que tiene que ser tipo “drill-down”, es decir, poder seleccionar unos de los objetos agrupados e ir filtrando el resultado en base a esta selección, hasta saber el detalle completo.

3.5. SEGURIDAD

Los equipos ofertados deben cumplir con los siguientes requerimientos mínimos en cuanto a funcionalidades relativas a seguridad:

36. Arquitectura basada en interfaces o zonas, para la aplicación de políticas de seguridad.

37. Posibilidad de agrupar interfaces del propio firewall en conjuntos independientes formando zonas, de forma que las políticas de seguridad se definan por zonas pudiendo incluir en las mismas políticas varias zonas origen y destino para el análisis de tráfico y procesado de reglas de seguridad, así como la posibilidad de crear múltiples reglas de seguridad entre zonas origen y destino o incluir cualquier zona origen o destino de tráfico en dichas reglas.

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

38. Se deberá poder analizar los ficheros comprimidos de diferentes formatos en busca de amenazas.

39. Posibilidad de definición de los tipos de datos en función de palabras clave, expresiones regulares, atributos de archivo y plantillas corporativas.

40. Monitorizar y controlar la navegación web pudiendo trabajar con listas blancas y negras.

41. Capacidad de requerir autenticación de múltiple factor en el acceso a cualquier servicio por distintas vías (token hardware o software, SMS, email, etc.) integrado en la misma plataforma de seguridad para la VPN y administradores del firewall.

42. Funcionalidad de reconocimiento del tipo de dispositivo del cliente (iPhone, iPad, Android, etc.) y poder hacer políticas en función del tipo de dispositivo, sin la instalación de ningún agente en el dispositivo remoto.

43. Funcionamiento como IPS basado tanto en patrones (basado en firmas con más de 7000 firmas prestablecidas) como en umbrales ("Rated based"). Posibilidad de crear firmas de IPS customizadas.

44. Definición de objetos para aplicación de políticas de seguridad, de diferentes tipos: IP, Subnet, intervalo de IPs, geografía y FQDN.

45. Detección y bloqueo de botnets en base a listas de reputación globales.

46. Inspección de certificados SSL.

47. Inspección de tráfico cifrado SSL

48. Capacidad para identificar las aplicaciones activas actuales (incluyendo aplicaciones Web 2.0)

49. La solución debe clasificar las aplicaciones en diferentes categorías y subcategorías, para poder aplicar reglas de acuerdo con estas categorías / subcategorías (control granular dentro de la aplicación).

50. Aplicar técnicas de identificación de aplicaciones a todos los puertos TCP / UDP y no sólo en los más comunes.

51. Capacidad para identificar las aplicaciones bajo túneles HTTPS (VPN SSL) e IPSec.

52. Capacidad de descifrar tráfico SSH y detectar aplicaciones no legítimas sobre este protocolo.

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

53. Capacidad de identificación de aplicaciones a nivel 7 así como la identificación de subfunciones dentro de una aplicación como por ejemplo “compartir escritorio de webex”, “chat dentro de webex”, “transferencia de ficheros en webex”, etc.

54. Posibilidad de agrupación de las aplicaciones por categorías, de forma que las políticas de seguridad sean aplicadas por categorías de aplicaciones.

55. Posibilidad de identificar aplicaciones propietarias que usen los protocolos HTTP y TCP.

56. Posibilidad de crear reglas de calidad de servicio según las aplicaciones que se usen en el tráfico, y los usuarios o grupos de usuarios que lo generen.

57. Posibilidad de aplicar diferentes perfiles de seguridad (IPS, Antivirus, Antispyware, Sandboxing, etc) para diferentes aplicaciones que funcionen por el mismo puerto.

58. Posibilidad de aplicar políticas de NAT de forma independiente a las políticas de seguridad ante vulnerabilidades y de protección de la red interna.

59. Posibilidad de habilitar todas las funciones de seguridad que ofrezca el equipo, sin penalización en rendimiento dependiendo del número de ellas habilitadas.

60. Posibilidad de descifrar tráfico cifrado y enviarlo en claro a otras soluciones para realización de sus funciones, y recibirlo nuevamente después para su envío a destino previa aplicación de las políticas de seguridad que correspondan en el firewall.

61. Utilización de motores propios de inspección para los servicios de seguridad (Antivirus, IPS, URL Filtering, Antimalware, etc.).

62. Posibilidad de definir aplicaciones y/o vulnerabilidades propias mediante diferentes parámetros como los puertos tcp o udp que se usan en dicha aplicación y combinaciones de patrones dentro de las cabeceras de los paquetes o en los propios payloads de dichos paquetes que se deben cumplir para que se reconozca la aplicación y/o vulnerabilidad.

63. Los firewalls ofertados deben tener la posibilidad de descifrar tráfico SSL y SSH de forma granular, de forma que se puedan establecer políticas de descifrado basándonos en las zonas por las que viaja el tráfico, según las direcciones ip origen o destino del tráfico enviado, los usuarios que generan dicho tráfico o los puertos que se están usando para el envío de tráfico, siendo posible excluir categorías de sitios de internet a descifrar.

64. Posibilidad de descifrar tráfico que pasa a través del firewall destinado a sitios web que utilicen certificados de curva elíptica (ECC).

65. Captura de tráfico. Los firewalls propuestos deben tener la capacidad de realizar

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

capturas del tráfico que atraviesa sus interfaces en formato PCAP, de forma que se puedan establecer criterios de la captura como capturar el tráfico originado por un cierto origen IP o destino, cierto puerto o también capturar tráfico de una aplicación en concreto independientemente del origen o destino del tráfico o incluso aplicar filtros de captura de tráfico exclusivamente cuando se detecte un virus o un ataque en los motores de protección.

66. El fabricante deberá disponer de un servicio de inteligencia de amenazas que en algún momento permita ampliar la plataforma ofreciendo visibilidad y contexto de las amenazas identificando autores, familias de malware, campañas, sectores objetivo, comportamientos maliciosos, exploits, etc.

67. En caso de que alguna característica ofrezca diferentes datos de rendimiento en los datasheets oficiales para diferentes escenarios, se considerará siempre el de peor valor en el entendimiento de que se puede requerir su uso en esas condiciones.

68. Deberá tener la capacidad de integrarse con soluciones que permitan procesar inteligencia de amenazas procedentes de feeds propios y de terceros, recogiendo, agregando y normalizando los Indicadores de compromiso (IoC) para hacerlos disponibles para su consumo en el propio firewall.

69. Deberá permitir el envío, ya descifrado, de la totalidad o de parte del tráfico cifrado que atraviese el firewall y que cumpla la política de seguridad configurada, hacia una cadena de soluciones de seguridad de terceros, estableciendo una cadena privada de inspección/análisis para aplicar funciones complementarias provistas por dichas soluciones.

70. Soporte de Proxy web nativo en el equipo.

71. Capacidad de bloquear ataques de día cero en línea mediante modelos de Deep Learning.

72. Detección de comandos y control (C2) evasivos en tiempo real.

73. Protección contra secuestro de DNS (DNS Hijacking) en tiempo real.

74. La solución propuesta debe integrar un servicio de seguridad IoT nativo que utilice aprendizaje automático (ML) en la nube para descubrir, clasificar e identificar de manera precisa todos los dispositivos conectados a la red, incluidos los dispositivos IoT no gestionados, sin necesidad de desplegar sensores físicos adicionales, ni agentes. La identificación no debe basarse únicamente en firmas estáticas o direcciones MAC (OUI), sino en el análisis del comportamiento del tráfico mediante modelos de Deep Learning para detectar anomalías y recomendar políticas de Zero Trust automáticamente basadas en el comportamiento observado del dispositivo.

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

3.5.1. *PROTECCIÓN ANTE ATAQUES DENEGACIÓN SERVICIO*

75. Los cortafuegos ofertados deben contar con medidas de protección ante ataques de Denegación de Servicios de forma que dichas medidas puedan ser activadas atendiendo a criterios como la zona o conjunto de interfaces desde donde se origina el tráfico, zona o conjunto de interfaces hacia dónde va dirigido el tráfico y pudiendo restringir dentro de estos interfaces las direcciones ip origen y destino a inspeccionar o el usuario o grupo de usuarios interno de la red que puede estar originando el ataque.

76. Se deberá contar al menos con los siguientes tipos de protección: SYN Flood, UDP Flood, ICMP Flood, ICMP Flood, protección ante inundaciones por nuevas sesiones, o protección por ataques de desborde por límites de sesiones establecidas, pudiendo en cada caso establecer los umbrales necesarios para activar dichas protecciones.

3.5.2. *PROTECCIÓN ANTE VULNERABILIDADES*

77. Los cortafuegos ofertados deben contar con la posibilidad de aplicar políticas de protección ante vulnerabilidades y exploits tanto al tráfico entrante como al saliente, debiendo cumplir con las siguientes funcionalidades:

78. Se debe poder aplicar políticas tanto de detección como de prevención (modo IDS o IPS) ante posibles exploits de vulnerabilidades que se detecten en el tráfico bien entrante o saliente de Internet sin incurrir en latencia superior a 1 milisegundo para no penalizar la sensación del usuario, efectuando el análisis en una única pasada para todo tipo de amenazas.

79. En la protección ante vulnerabilidades el criterio a usar es la identificación de la aplicación que se usa para poder aplicar perfiles de vulnerabilidades ajustados a dicha aplicación, de forma que las prestaciones de los equipos no se vean mermadas.

80. El fabricante deberá disponer de un servicio de inteligencia de amenazas que en algún momento permita ampliar la plataforma ofreciendo visibilidad y contexto de las amenazas identificando autores, familias de malware, campañas, sectores objetivo, comportamientos maliciosos, exploits, etc.

81. Los perfiles de detección y protección ante vulnerabilidades deben permitir ser aplicados tanto para el tráfico originado desde la red interna como para el tráfico originado desde Internet, debiendo ser posible la aplicación de detección y protección ante vulnerabilidades especificando si son vulnerabilidades que aplican a los clientes, los servidores o a ambos indistintamente.

82. Las vulnerabilidades deben estar categorizadas por tipos y por niveles de riesgo, de

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

forma que la aplicación de perfiles de protección en el tráfico se pueda realizar en base a estas categorías.

83. Se debe poder permitir usar la identificación CVE de vulnerabilidades para poder usar dicha identificación en la aplicación de perfiles de protección específicos.

84. Utilización de la identificación de aplicaciones como criterio para seleccionar los perfiles de protección de vulnerabilidades, de forma que se apliquen solo aquellas firmas específicas según la aplicación que se está utilizando.

3.5.3. FILTRADO DE URL

Los equipos ofertados deben tener la posibilidad de filtrar la navegación http o https según la URL que se desea visitar basándose en diferentes criterios:

85. Posibilidad de definir manualmente listas estáticas de URLs o de IPs permitidas y no permitidas para la navegación, con posibilidad de definir para las no permitidas la acción a realizar (bloquear, permitir pero advertir, generar solamente un log, etc.).

86. Permitir la navegación basándose en categorías de URL, siendo dichas categorías actualizadas periódicamente a través de un servicio en la nube que permita al menos categorías de URL como "malware", "phishing", "command-and-control", "hacking", etc.

87. Posibilidad de incluir listas dinámicas, de forma que los equipos puedan ser configurados para que de forma periódica consulten fuentes de inteligencia propios o de terceros con IoCs maliciosos, y permita automatizar la denegación del tráfico hacia/desde estos IoCs en la política del firewall. El fabricante deberá proporcionar listas de IP maliciosas que se actualicen y mantengan automáticamente.

88. Posibilidad de detectar el robo y envío de credenciales corporativas (usuarios y password de la red corporativa) hacia las webs que se visitan, de forma que se pueda advertir, bloquear o permitir dicho envió de credenciales en función de las categorías de web visitadas.

89. Estas posibilidades deberán poder ser configurables mediante perfiles de forma que se puedan aplicar dichos perfiles a las reglas de tráfico tanto saliente como entrante de forma granular, permitiendo dicha aplicación a ciertos tipos de tráfico y no a otros.

3.5.4. ANTIMALWARE

Los equipos ofertados deben tener la capacidad de detectar mediante firmas, a los posibles equipos comprometidos en la red que intenten establecer comunicación con servidores de comando y control, permitiendo realizar acciones predeterminadas como bloquear o monitorizar y registrar mediante log, este tipo de tráfico.

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

90. Los cortafuegos propuestos deben tener la capacidad de definir políticas de antivirus, de forma que las descargas de ficheros realizadas en sentido Internet a red Interna o viceversa sean inspeccionadas y bloqueadas si su contenido es malicioso.

91. Se debe poder aplicar políticas que permitan aplicar el motor de antivirus sobre protocolos como FTP, HTTP, IMAP, POP3 y SMTP, definiendo para cada uno de estos protocolos la acción a realizar (permitir los ficheros, descartar los ficheros, desconectar la sesión o registrar mediante logs) ante la detección del fichero malicioso por el motor de antivirus, adicionalmente, se debe poder tener la posibilidad de enviar el fichero que se inspecciona a un servicio en Internet que permita el análisis de dicho contenido y emita un veredicto en caso de que el fichero sea malicioso que permita realizar al cortafuegos las acciones oportunas.

92. Los cortafuegos deben permitir la aplicación de políticas de antivirus de forma granular, permitiendo por ejemplo la aplicación de dichas políticas a ciertos usuarios de determinados grupos o a ciertos segmentos de red con determinado direccionamiento o a ciertas aplicaciones.

3.5.5. BLOQUEO DE FICHEROS Y DATOS SENSIBLES

93. Los cortafuegos propuestos deben tener la capacidad de identificar ficheros no basándose en el tipo MIME del archivo y no en su extensión, permitiendo al menos **50 tipos de ficheros identificables**.

94. Se debe poder aplicar políticas de bloqueo de ficheros basándose en su nombre o en su tipo, de forma que se pueda bloquear descargas de ciertos tipos de fichero o se permita su descarga pidiendo confirmación al usuario y se generen los logs correspondientes.

95. Los equipos propuestos deben poder ser capaces de aplicar políticas de bloqueo de ficheros atendiendo a criterios como origen y destino del tráfico, usuarios o grupos que originan las descargas, tipo de aplicación o de tráfico que genera las descargas de fichero y para el caso de navegación en internet se debe poder bloquear las descargas de ficheros cuando dicha navegación sea hacia URL categorizadas como peligrosas o que puedan suponer amenazas de seguridad.

96. Prevención contra fugas de información (Data Lost Prevention-DLP). Los equipos deben tener la capacidad de búsqueda de patrones sensibles como DNI, tarjetas de crédito, etc., así como a asociaciones concretas.

3.5.6. TECNOLOGÍA DE SANDBOXING

97. Los cortafuegos propuestos deben tener la capacidad de disponer de un servicio en la nube capaz de analizar ficheros de tipo desconocido o enlaces URL recibidos en

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

correos electrónicos, de forma que se permita el envío de dicha información para análisis atendiendo a criterios como:

- Tipo de aplicación que se está usando para transferir el fichero.
- Tipo de fichero que se está transfiriendo.
- Dirección de transferencia (descarga o subida de ficheros).

98. El servicio en la nube será capaz de analizar los siguientes tipos de ficheros: paquetes de aplicaciones Android, ficheros flash, applets java, ficheros de Microsoft office, ficheros ejecutables con formato PE incluyendo DLL, ficheros PDF y enlaces HTTP y HTTPS incluidos en correos electrónicos recibidos por SMTP y POP3.

99. El análisis realizado por este servicio en la nube, en caso de que la muestra enviada sea categorizada como de tipo malicioso por suponer un riesgo de seguridad, deberá generar las firmas apropiadas en un plazo máximo de 5 minutos que se utilizarán para actualizar los motores propios de antivirus y filtrado URL de forma que las posteriores descargas de los mismos ficheros o URL enviadas sean bloqueadas por dichos firewalls. Además, el firewall también se aprovechará, en el mismo plazo de tiempo, de la inteligencia generada para cualquier muestra analizada en dicho servicio incluso procedente de otros clientes u otras fuentes externas.

100. Los firewalls deben tener la capacidad de enviar también al servicio de sandboxing en la nube no solamente aquellos ficheros de tipo sospechoso sino aquellos que hayan sido bloqueados por su propio sistema de firmas, con objeto de poder analizar variantes de malware e incorporar esas variantes al sistema de firmas de los propios motores del equipo. Además, se deberá poder consultar la información enviada y evaluada en la nube a efectos de generar los informes correspondientes.

101. Para satisfacer el RGPD (Reglamento General de Protección de Datos), el servicio en la nube debe estar disponible en territorio de la Unión Europea.

3.5.7. PROTECCIÓN FRENTE AL PHISHING

102. Prevención frente al phishing de credenciales corporativas: capacidad de monitorización y bloqueo del uso de las credenciales corporativas en cualquier sitio web que no sea de confianza.

103. Capacidad de URL Filtering de forma que se detecten urls maliciosas utilizando diversas técnicas, incluyendo mecanismos de IA y/o Machine Learning que permitan comparar un sitio web con el que pretende suplantar para determinar rápidamente si se trata de un sitio de phishing o no, procediendo al bloqueo inmediato.

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

104. Capacidad de extraer los enlaces http/https de un correo electrónico, analizarlos y determinar automáticamente si se trata de un phishing o no, para poder bloquear un posterior acceso a dicho sitio.

105. Capacidad de prevención frente al phishing, a través de la resolución DNS del FQDN del sitio en cuestión.

3.6. ACCESO REMOTO VPN

106. Acceso remoto seguro mediante redes privadas virtuales (VPN) con autenticación multifactor (MFA).

107. El dispositivo dispondrá de VPN SSL y 9 Gbps de rendimiento IPSec (paquetes de 512 bytes).

108. El dispositivo admitirá como mínimo 1.800 usuarios concurrentes PN SSL sin licencias adicionales.

109. El sistema propuesto deberá cumplir los estándares de la industria, sin el apoyo externo adicional de hardware o módulos:
   a. IPSEC VPN (IPv4 e IPv6)
   b. SSL VPN

110. Capacidad de realizar VPN “Site to Site” o “SSL VPN”

111. Clientes propios VPN para dispositivos Linux, IOS y Android.

3.7. ALTA DISPONIBILIDAD

112. Failover Activo / Pasivo, Activo / Activo sin necesidad de licencia adicional.

113. Sincronización de configuración y sesiones.

114. Interfaces reservados para gestión.

115. Posibilidad de configurar interfaces HeartBeat redundantes.

3.8. BALANCEO ACCESO INTERNET

116. El sistema debe ser capaz de realizar balanceo de carga de los enlaces de Internet de forma dinámica con diversos métodos.

117. El sistema debe ser capaz de proporcionar redundancia de enlaces WAN

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

monitorizando el estado de las líneas.

3.9. IDENTIFICACIÓN DE USUARIOS

Cada firewall ofertado deberá tener las siguientes características técnicas relativas a gestión e identificación de usuarios, entendiéndose como funcionalidades mínimas a cumplir:

118. Identificar usuarios, integrándose con los sistemas de identificación de la UBU (Microsoft Active Directory, ClearPass, LDAP, SAML, etc.)

119. Control de usuarios de Citrix y de Microsoft Terminal Server, para la identificación unívoca de los usuarios a partir del tráfico generado desde estos sistemas.

120. Soporte de mensajes Radius Accounting para SSO.

121. Autenticación en servidores remotos mediante LDAP, RADIUS y TACACS+

122. Capacidad de poder identificar usuarios en la VPN haciendo uso de protocolos como Kerberos, NTLM, ClearPass, LDAP, SAML SSO, TACACS+, RADIUS, Certificados de Cliente o autenticación local.

123. Capacidad de analizar mensajes de syslog con información de login y logout para identificación de usuarios.

3.10. GESTIÓN Y ADMINISTRACIÓN

Cada firewall ofertado deberá tener las siguientes características técnicas relativas a gestión y administración de la propia plataforma, entendiéndose como funcionalidades mínimas a cumplir:

124. Soporte de SNMP de los datos básicos del equipo (CPU, Memoria, disco, etc.). Integración con Zabbix.

125. Envío de logs vía SYSLOG, para retención y posterior tratamiento, con posibilidad de envió de logs selectivos según niveles de severidad y también según atributos como por ejemplo los tipos de amenaza.

126. Administración por GUI y CLI directamente en el equipamiento, sin necesidad de instalar un cliente específico en máquina externa al firewall para su administración y / o cualquier otra función del firewall.

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

127. Creación de perfiles y roles de administración con diferentes niveles de privilegio para poder administrar ciertas funcionalidades.

3.11. INFORMES

128. Los firewalls proporcionados deben tener la capacidad de generar informes tanto predefinidos como personalizados utilizando los logs generados.

129. Se debe poder crear y programar informes personalizados que muestren exactamente la información que desea ver mediante el filtrado de condiciones y columnas para incluir. También se podrá incluir constructores de consultas para obtener un desglose más específico de los datos del informe.

130. Los informes se podrán generar a demanda, de forma recurrente y se podrán programar para su entrega por correo electrónico. Se podrá definir el intervalo de fechas entre las cuales se desea la información de dicho report, dentro de las limitaciones de almacenamiento de los propios equipos.

131. Grupos de informes: Capacidad de combinar distintos informes personalizados y predefinidos, en un único documento con formato PDF que se podrá enviar por correo electrónico a uno o más destinatarios.

132. Se deberá disponer de informes de la actividad por usuario, incluyendo aplicaciones utilizadas, sitios web visitados, anchos de banda consumidos por las diferentes aplicaciones, informes sobre los orígenes y destinos geográficos de las amenazas detectadas, informes sobre el análisis de comportamiento de tráfico observado que permita detectar equipos comprometidos, etc.

133. Al finalizar la implantación se tendrán disponibles los siguientes informes:

a. **Resumen del estado de la red** (con las categorías de amenazas, aplicaciones, tendencias, tráfico y filtrado de URL).
b. **Actividad de usuarios o grupos,** en concreto en la red de gestión.
c. **Informes de botnet:** identificando los posibles hosts infectados por botnets en la red.

4. SERVICIOS

Dentro de este apartado se consideran incluidos todos los trabajos que deba realizar el adjudicatario para proporcionar una solución “llave en mano” con los componentes y arquitectura propuesta:

a) Instalación física de todo el equipamiento y componentes, configuración a nivel de red, gestión, almacenamiento, etc. y su puesta en marcha.

b) Instalación de la plataforma de gestión centralizada.

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

c) Cableado, etiquetado y conexionado de los puertos del equipamiento ofertado.

d) Elaboración del Plan de migración de servicios de acuerdo con el área de Comunicaciones del Servicio de Informática y Comunicaciones (SIC).

e) Migración de todas las reglas y configuraciones de los firewalls actuales al nuevo equipamiento.

f) Actualización de los equipos a nivel de parches.

g) Configuración de una solución de copia de seguridad de todos los sistemas requeridos.

h) Configuración de una solución de Disaster Recovery.

i) Pruebas de carga y ajuste de los parámetros necesarios para el funcionamiento óptimo de la instalación.

j) Retirada, destrucción de la información y posterior reciclaje del equipamiento antiguo sustituido en este contrato, que deberá acreditarse mediante certificación.

k) Implementar una política de archivado y protección de logs adecuada, en función de los parámetros especificados por la universidad.

l) Implantar las medidas de seguridad para el cumplimiento del ENS de forma conjunta con los técnicos de la universidad.

m) Formación según lo indicado en el apartado **6 de este PPT.**

n) Documentación según lo indicado en el apartado **7 de este PPT.**

o) Servicios de soporte y mantenimiento según lo indicado en el apartado **8 de este PPT.**

5. PLAN DE IMPLANTACIÓN DEL EQUIPAMIENTO SUMINISTRADO

Será necesario incluir en la documentación técnica el **Plan de Implantación** que especifique el plan de proyecto para la instalación y configuración del suministro y la migración de todos los servicios actuales de la UBU a las nuevas infraestructuras, siguiendo las cláusulas técnicas especificadas en este Pliego de prescripciones técnicas (PPT).

El plazo máximo para la recepción, instalación, configuración y puesta en marcha del equipamiento, incluyendo la migración de los servicios objeto de este pliego, **será el 31 de agosto de 2026**. Una vez firmada el acta de recepción, a la finalización de la implantación, empezará a contar el periodo de mantenimiento **hasta un máximo de 5 años desde la firma del contrato**.

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

Todos los elementos suministrados, tanto los explícitamente requeridos en este pliego como aquellos que sin estarlo faciliten y garanticen la funcionalidad descrita en este documento pasarán a ser propiedad de la UBU.
Con el fin de minimizar el impacto en los servicios de la UBU, la puesta en producción deberá realizarse necesariamente durante el mes de agosto de 2026 evitando cortes de servicio en los meses anteriores y posteriores.

Es parte fundamental del objeto del contrato la migración de todas las configuraciones actuales y la información de seguridad, así como la integración con otros subsistemas (SIEM, ClearPass, Active Directory, SSO, Zabbix, etc.).

El Plan de Implantación contendrá la planificación detallada de las actuaciones requeridas hasta la puesta en marcha del equipamiento objeto de este pliego, incorporando los siguientes puntos:

5.1. FASES DEL PROYECTO

a. Planificación temporal del proyecto.
b. Desglose de las tareas a realizar en cada fase y responsables de cada una de ellas.
c. Establecimiento de los protocolos y periodos de pruebas de servicio.

La transición del servicio, deberá realizarse de la forma más armónica y transparente posible para la Universidad. Se requiere plantear una estrategia de implantación que permita minimizar el tiempo de parada de los servicios para realizar la migración de los mismos a las nuevas infraestructuras. **Cualquier tarea que implique una interrupción o merma en la disponibilidad del servicio deberá realizarse, en la medida de lo posible, en festivos u horarios de baja actividad de la Universidad, de forma que se minimice el impacto en los servicios.**

5.2. EQUIPO DE TRABAJO

Los técnicos participantes en el proyecto deberán estar certificados por los fabricantes de las tecnologías utilizadas en este proyecto. Se entregará un resumen de las acreditaciones y certificaciones técnicas del personal, detallando el perfil profesional de los técnicos asignados al proyecto, su relación con la empresa y su dedicación al proyecto.

6. FORMACIÓN

Al inicio del contrato y posteriormente cada de año de mantenimiento se ofertarán **cursos oficiales de los fabricantes en las tecnologías objeto del contrato con un mínimo de 20 horas de formación anuales online o in-situ en la Universidad** (repartidas en cuatro jornadas), destinadas al personal técnico de la universidad. En la oferta deberán explicitarse las horas y el temario propuesto.

Además, se requieren al menos **dos jornadas in-situ**, impartidas por el responsable del despliegue explicando la solución instalada y su configuración, que se impartirán al finalizar la implantación. Previamente a esta formación, la empresa adjudicataria deberá

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

haber proporcionado al personal del SIC toda la documentación relativa a la solución implantada.

Una vez transcurrido un tiempo **mínimo de 4 meses** después de la instalación, se impartirán otras **dos jornadas in-situ**, para afinar la solución y aclarar las dudas y problemas que puedan haber surgido en ese período.

Posteriormente, **con periodicidad anual se dedicará al menos una jornada in-situ** de un técnico de la empresa adjudicataria, para revisar el estado de la instalación y aclarar las dudas y problemas que hayan surgido.

7. DOCUMENTACIÓN

El proyecto habrá de generar, como mínimo, la siguiente documentación que deberá ser entregada a la UBU a la finalización de la implantación y convenientemente actualizada y proporcionada a la universidad de forma periódica, **como mínimo anualmente**.

- Arquitectura del sistema.
- Documento de diseño técnico detallado de la solución global implantada.
- Descripción de las configuraciones de cada uno de los subsistemas.
- Manuales del diferente equipamiento incluido en la infraestructura.
- Manuales de usuario para la conexión a la VPN personalizados para UBU.
- Mecanismos y parámetros acordados para medir el rendimiento de los diversos componentes.
    - Protocolos de actuación: procedimientos de operación: arranque y parada del sistema, copias de seguridad y restauración, envío de logs al SIEM.
    - Comunicación de incidencias: descripción de los procedimientos de escalado de incidencias. Mecanismos de respuesta a incidencias (telefónica, servicio de soporte online, etc.).
    - Gestión de cambios y configuraciones.
    - Monitorización y gestión de la seguridad.

Toda la documentación deberá entregarse en formato electrónico, generado con herramientas ofimáticas estándar del mercado (PDF, Word, ODT).

8. CONDICIONES DEL SERVICIO DE SOPORTE Y MANTENIMIENTO

Una vez firmada el acta de recepción a la finalización de la instalación, configuración y puesta en marcha de los servicios, la empresa adjudicataria deberá prestar el servicio de soporte y mantenimiento.

La empresa adjudicataria deberá garantizar el correcto funcionamiento del equipamiento objeto del contrato, poniendo los medios necesarios para la resolución de los problemas, errores y fallos de funcionamiento, que le comuniquen los interlocutores designados por la Universidad de Burgos, sin que represente coste alguno para la Universidad.

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

8.1. *ALCANCE*

Dentro del alcance de este contrato se incluirán todas las actuaciones y el soporte necesario para que las infraestructuras objeto del mismo, se mantengan en funcionamiento, tanto en la operativa diaria, como en la incorporación de nuevas funcionalidades y/o cambios en la topología o configuración, así como en las sucesivas actualizaciones del firmware, parches o nuevas versiones del software.

Con carácter general, la Universidad de Burgos dispondrá de soporte con los servicios siguientes:

a) Consultoría y asistencia técnica, **en idioma castellano**, para atención de incidencias, corrección de errores y problemas de funcionamiento de los sistemas objeto del contrato (paradas, indisponibilidad total/parcial del servicio, pérdidas de rendimiento, fallos hardware, etc.), detectados por la empresa o comunicados por los responsables de la Universidad de Burgos.
b) Monitorización remota de equipos.
c) Generación de informes de seguimiento del contrato y elaboración de actas de las reuniones.
d) Suministro, instalación y configuración de todas las actualizaciones de firmware, parches o nuevas versiones del software o incorporación de mejoras o nuevas funcionalidades, liberadas por el fabricante.
e) Asesoramiento a los técnicos del Área de Comunicaciones de la UBU (a petición de la universidad y con cargo a la bolsa de horas ofertada).
f) Realización de tareas habituales de operación de las infraestructuras (a petición de la universidad y con cargo a la bolsa de horas ofertada).
g) Revisiones periódicas del equipamiento objeto del contrato y propuestas de mejora (a petición de la universidad y con cargo a la bolsa de horas ofertada).

La Universidad facilitará un acceso remoto individual a cada una de las personas del equipo de soporte de la empresa adjudicataria, a efectos de que pueda realizar el diagnóstico y la solución de incidencias, el seguimiento y supervisión de los parámetros de rendimiento y disponibilidad, y las modificaciones del firmware, software, configuración, consultas, ajustes, y en general, para cualquier tarea indispensable para el cumplimiento de las cláusulas previstas en este pliego.

La empresa adjudicataria dispondrá de **una herramienta web disponible en 24*7 para el registro, seguimiento y control de las incidencias**, peticiones, consultas e intervenciones realizadas y su situación. Adicionalmente la comunicación de incidencias y solicitudes por parte de la Universidad de Burgos podrá ser realizada a través de correo electrónico o vía telefónica, debiendo quedar registradas en el portal web.

El licitador deberá presentar claramente en su oferta los mecanismos para la comunicación de las incidencias, el horario laboral efectivo de prestación del servicio, los tiempos de respuesta y resolución, así como los recursos técnicos y humanos de que dispone.

Durante la ejecución de los trabajos, el adjudicatario se compromete a facilitar en todo

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

momento, la información y la documentación que dicho personal solicite para disponer de un pleno conocimiento de las circunstancias en que estos se desarrollan, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

El soporte prestado incluirá obligatoriamente los siguientes servicios:

8.2. ATENCIÓN DE AVERÍAS E INCIDENCIAS

Servicio de asistencia técnica con el fin de detectar y solucionar las incidencias que se presenten en el equipamiento objeto del presente contrato, incluyendo, en su caso, los desplazamientos que se deban realizar. En todos los casos se incluye la intervención en el lugar de instalación de los equipos, en caso de que el personal del SIC lo considere necesario para la buena resolución de la avería.

La empresa adjudicataria deberá garantizar, la previsión y disponibilidad de cualquier clase de repuesto necesario para el mantenimiento de los equipos, explicitando documentalmente en su oferta la existencia de repuestos de dichos equipos.

Si se produjese una avería de hardware, se suministrarán e instalarán por parte de la empresa adjudicataria los elementos necesarios para su reparación. En el caso de que se haga necesaria la retirada del equipo averiado, se proporcionará para su sustitución, **un equipo nuevo del mismo modelo y fabricante**. El transporte y la reposición de piezas, se realizará sin coste adicional para la UBU. Estos elementos pasarán a ser propiedad de la Universidad, al tiempo que los sustituidos pasarán a propiedad del adjudicatario. Cuando se proceda a la sustitución de cualquier equipo, la empresa adjudicataria realizará una reinstalación del software y de los ficheros de configuración propios del equipo original.

Ante la imposibilidad de conseguir un equipo idéntico al original, por causas de fuerza mayor (obsolescencia, descatalogación, etc.), lo pondrá en conocimiento del SIC, quien evaluará la conveniencia o no de su sustitución por un equipo de características y funcionalidades equivalentes. En caso afirmativo se suministrará un equipo con funcionalidades idénticas o superiores y se deberá realizar la adaptación de los ficheros de configuración del equipo original al nuevo equipo. El equipo deberá ser configurado por la empresa de manera que pueda prestar todas las funcionalidades que se encontraban operativas en el equipo averiado antes del fallo, salvo que se acuerde lo contrario si las circunstancias lo desaconsejasen.

Todas las versiones y actualizaciones del software estarán incluidas en el alcance del contrato y serán gratuitas para la UBU. En el caso de producirse el fallo de un equipo por un error de su software interno, deberá proveerse a la Universidad de Burgos de la actualización correspondiente. La versión de software que se suministre deberá ser compatible con las funcionalidades operativas en el equipo averiado antes del fallo. La empresa adjudicataria será responsable de la configuración del mismo con la nueva versión.

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

La oferta deberá incluir la provisión de servicios de monitorización, actualización y configuración remota de equipos, siendo por cuenta del adjudicatario todo el equipamiento necesario para los mismos. Durante el proceso de diagnóstico y resolución de problemas de manera remota, la Universidad de Burgos colaborará con la empresa adjudicataria:

- Facilitando toda la información necesaria para que la empresa preste el soporte remoto, puntual y profesionalmente.
- Realizando las actividades razonables para ayudar a identificar o resolver el problema.

8.3. SOPORTE DEL FABRICANTE

La empresa adjudicataria deberá acreditar **contratos de mantenimiento en vigor, en 24*7, con el fabricante**, durante toda la duración del contrato.

La empresa adjudicataria escalará al servicio técnico del fabricante aquellas incidencias que la propia empresa o la UBU consideren necesarias, sin coste adicional. La empresa adjudicataria será la encargada de gestionar las incidencias software y/o hardware con el fabricante de los elementos objeto del contrato.

La empresa adjudicataria garantizará el acceso web privilegiado del personal del Área de Comunicaciones del SIC, a la página de soporte del fabricante de los equipos objeto del presente contrato, para la consulta de información técnica, descarga de software o el seguimiento de los casos abiertos con el fabricante.

Dentro del alcance se incluye el suministro, sin coste adicional, a petición de la Universidad, de las nuevas versiones de los programas asociados a los equipos que el fabricante de los mismos pueda sacar al mercado durante el período de vigencia del contrato, así como su documentación. La empresa adjudicataria deberá mantener informada puntualmente a la Universidad de la aparición de las nuevas versiones.

8.4. MANTENIMIENTO PREVENTIVO

Una vez implantada la solución se establecerá un calendario para efectuar un seguimiento de todos los componentes de la instalación, realizando un análisis del rendimiento de los sistemas para certificar que la configuración es idónea.

Entre las acciones de mantenimiento preventivo se incluye la monitorización remota **24x7** de las infraestructuras objeto del contrato y la configuración, en colaboración con el Área de Comunicaciones del SIC, de alertas de malfuncionamiento de los sistemas, que permitan la detección automática de problemas y reducir los fallos de disponibilidad de los servicios.

Los servicios estarán monitorizados de forma continua, al menos de dos maneras:

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

- Monitorización "end-to-end" o experiencia de usuario: verificando el correcto funcionamiento del sistema.
- Monitorización de los componentes hardware de la infraestructura.

Cuando se reciban alertas detectadas por los mecanismos de monitorización, se deberán crear los registros de incidencias oportunas para su resolución lo antes posible, según los términos de soporte descritos.

Dentro del mantenimiento preventivo también se incluirá por parte del adjudicatario la subsanación de las vulnerabilidades de seguridad detectadas en los componentes de la solución ofertada, la actualización de versiones tanto del firmware como del software de los equipos a solicitud de los técnicos de la Universidad, así como la actualización de los equipos a nivel de parches. En este apartado es importante señalar que, si el software utilizado en los equipos requiere del pago de una licencia software anual, ésta correrá a cargo de la empresa adjudicataria.

Es responsabilidad de Universidad de Burgos permitir la instalación de las actualizaciones críticas de firmware que el equipo de soporte recomiende, así como las piezas y unidades de recambio que se le entreguen como parte del proceso de resolución de una incidencia, siempre con el condicionante de evitar o minimizar las paradas de los servicios.

8.5. SOPORTE AL PERSONAL DEL SIC

En la oferta se incluirá como **mínimo una bolsa de 50h anuales**, para la atención al personal del Área de Comunicaciones del SIC, **una vez finalizada la implantación**, al que puedan dirigirse para el planteamiento de cuestiones relacionadas con configuraciones, funcionalidades del equipamiento, diseño de nuevas soluciones y/o servicios etc. y que actúe como servicio de soporte para las tareas habituales de operación de las infraestructuras de la Universidad objeto del contrato.

Se requiere poner a disposición del contrato, como mínimo, un director de proyecto y dos técnicos de Comunicaciones con titulación universitaria, con experiencia acreditada mediante certificaciones de los fabricantes en las tecnologías objeto del contrato, y que hayan participado en, al menos, durante los últimos 3 años en proyectos similares.

La UBU deberá poder contar siempre con soporte especializado por parte de la empresa adjudicataria, por lo que ésta deberá **asignar un técnico cualificado principal y otro de respaldo,** para resolver problemas y asesorar al personal del SIC de la UBU sobre la correcta configuración del equipamiento objeto del contrato, en el supuesto que se necesite desplegar un nuevo servicio o se requiera una modificación, ampliación, o mejora de los servicios prestados.

La cuantificación en horas, así como la fecha límite de las actuaciones solicitadas por la Universidad, serán convenidos entre la empresa adjudicataria y la Universidad.

Dentro del alcance de este servicio se incluye la instalación y configuración, a petición de la Universidad, de los parches o nuevas versiones de los programas asociados a los

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

equipos que la compañía fabricante de los mismos pueda sacar al mercado durante el período de vigencia del contrato, así como su documentación.

9. ACUERDOS E INDICADORES DE NIVEL DE SERVICIO

9.1. *HORARIOS DE ATENCIÓN*

El servicio de comunicación de incidencias online tendrá una cobertura 24x7: es decir el servicio estará disponible las 24 horas del día, de lunes a domingo, incluidos los días festivos.

El horario laboral de prestación del servicio de mantenimiento es el intervalo de tiempo durante el cual se registrarán las llamadas y se prestará el servicio en las instalaciones de la Universidad o de manera remota.
El horario laboral será como mínimo de lunes a viernes de 8:00 a 18:00h.

Se podrá comunicar un número de incidencias ilimitado dentro de la duración del contrato.

9.2. *TIEMPOS DE RESPUESTA Y RESOLUCIÓN*

Se define el **tiempo de respuesta** como las horas que transcurren desde la comunicación de una incidencia por parte de la universidad hasta que se inicia la intervención por parte del técnico asignado por la empresa adjudicataria.

Se define el **tiempo de resolución** como las horas que transcurren desde que se notifica una incidencia por parte de la universidad, hasta que se repone el funcionamiento normal, aunque sea con una solución provisional

El **tiempo de respuesta hardware in-situ** es el que transcurre desde que la empresa adjudicataria recibe y registra la solicitud de servicio de hardware, hasta el momento en que un representante autorizado llega a las instalaciones de Universidad de Burgos.

El tiempo requerido de respuesta hardware in-situ para la asistencia que suponga interrupciones del servicio es de 4 horas. Para aquellas incidencias que no supongan pérdida de servicio el tiempo de respuesta será 8x5xNBD. Para cumplir este requisito se podrá contar con soporte del fabricante o establecer algún mecanismo adicional que lo cumpla.

El adjudicatario podrá iniciar y realizar diagnósticos remotos utilizando herramientas electrónicas de soporte remoto para acceder a los equipos cubiertos por el servicio, o bien utilizar otros medios disponibles para facilitar la resolución remota del problema. P**ara aquellos problemas técnicos que no se puedan resolver de modo remoto, un técnico autorizado de la empresa adjudicataria acudirá a las instalaciones de Universidad**

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

de Burgos en el período establecido de 4 horas, con el fin de prestar asistencia técnica para el producto de hardware cubierto y reparará o sustituirá componentes o el equipo completo, según sea necesario, para restablecer el funcionamiento normal del equipo.

Cuando el técnico autorizado de la empresa adjudicataria llegue a las instalaciones de Universidad de Burgos, seguirá prestando el servicio, bien in-situ o de forma remota, hasta que se restablezca el funcionamiento de los productos de hardware o mientras se logren avances razonables en su reparación.
Como parte del proceso de resolución, el especialista podría proponer a la Universidad de Burgos la instalación de mejoras disponibles y recomendadas para evitar la repetición del problema, garantizar el correcto funcionamiento de los productos de hardware, aumentar su rendimiento y mantener la compatibilidad con las piezas hardware de repuesto suministradas.

Los tiempos de respuesta y resolución (de incidencias no hardware y peticiones), dependerán de su prioridad, según los criterios que se indican a continuación:

- **Prioridad 1 (Crítica):** El equipamiento está fuera de servicio o degradado de forma que impide la realización del trabajo afectando a la disponibilidad de los servicios críticos de la universidad (red, correo, UBUVirtual, matrícula y página web). El tiempo de respuesta máximo deberá ser de **2 horas** y el de resolución de **6 horas (como máximo)**, a partir de la comunicación de la avería.

- **Prioridad 2 (Urgente):** El sistema no funciona a pleno rendimiento, pero sigue siendo operativo. El tiempo de respuesta máximo deberá ser de **2 horas laborables** y el de resolución de **6 horas laborables** (como máximo), a partir de la comunicación de la avería.

- **Prioridad 3 (Ordinaria):** Mal funcionamiento del sistema que presenta problemas de efecto limitado o poco importante. El tiempo de respuesta máximo deberá ser de **2 horas laborables** y el de resolución de **8 horas laborables** (como máximo), a partir de la comunicación de la avería.

- **Otras peticiones:** En general todas aquellas incidencias o peticiones que pueden ser planificadas, estudiadas o consideradas dentro de unos plazos razonables, y con suficiente antelación para poder realizar un análisis de su implementación. Los tiempos de resolución de acordarán entre la universidad y la empresa adjudicataria. Si la Universidad de Burgos solicita un servicio programado, el compromiso de tiempo de resolución contará a partir de la hora de inicio acordada para llevar a cabo la tarea y se medirá respecto al tiempo acordado previamente. El tiempo de respuesta no será aplicable.

9.3. DISPONIBILIDAD DEL SISTEMA

Eliminando aquellos fallos que puedan ser imputables a la Universidad, se requiere:

Porcentaje de disponibilidad del servicio: **99,98% (medido mensualmente).**

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

9.4. *RENDIMIENTO*

Se entiende un rendimiento aceptable como aquél que permite el funcionamiento normal con todas las funciones previstas en este PPT, con tiempos de respuesta considerados como aceptables en sistemas similares y en entornos de explotación homólogos.

La Universidad y la empresa adjudicataria acordarán mecanismos y parámetros para medir el rendimiento, que serán validados al inicio del contrato y serán verificados en las sucesivas actualizaciones.

La empresa adjudicataria deberá implantar mecanismos de seguimiento y supervisión para garantizar el buen funcionamiento y rendimiento del sistema, tanto bajo la carga habitual de usuarios de la Universidad como en los períodos de más carga. Ambas partes se comprometen a informar a la otra de cualquier incidencia que pueda suponer o haya supuesto una disminución del rendimiento.

La empresa adjudicataria deberá definir los distintos grados de escalabilidad de la solución, de tal forma que sea previsible y valorable la inversión o modificaciones en la infraestructura necesaria para aumentar el volumen de entidades a tratar (datos, usuarios, etc.) y/o para mejorar el rendimiento.

9.5. *INDICADORES Y ACUERDOS DE NIVEL DE SERVICIO*

Indicador	Descripción	Valor Objetivo
Porcentaje de incidencias resueltas en plazo.	Porcentaje de incidencias que se resuelven dentro de los tiempos de resolución establecidos en función de los niveles de criticidad especificados. **Se medirá de forma mensual.**	**>95%**
Porcentaje de averías hardware resueltas en plazo	Porcentaje de averías hardware que supongan interrupciones del servicio resueltas en 4 horas. **Se medirá de forma mensual**.	**>95%**
Porcentaje de disponibilidad	Porcentaje de disponibilidad del servicio. **Se medirá de forma mensual.**	**>99,98%**
Porcentaje de rendimiento aceptable	Porcentaje de rendimiento aceptable del servicio. **Se medirá de forma mensual.**	**>99%**

Para facilitar el seguimiento, la empresa adjudicataria deberá entregar **informes mensuales con el grado de cumplimiento de los Acuerdos de Nivel de Servicio**, **así como la relación de las incidencias y actuaciones registradas durante ese periodo y el estado de la bolsa de horas**. En esos informes se detallará el tipo de incidencia, los momentos de apertura y cierre de las mismas, los tiempos de respuesta y resolución, las soluciones propuestas y las realmente llevadas a cabo junto con todos aquellos aspectos que deban destacarse, así como todas las actuaciones realizadas durante el período

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

considerado. Igualmente, en el caso de que se hayan llevado a cabo recomendaciones o acciones de tipo preventivo, se harán constar en dicho informe.

10. RESPONSABILIDADES EN DECISIONES TÉCNICAS

El personal del Área de Comunicaciones del S.I.C. es responsable del óptimo funcionamiento de las infraestructuras objeto del contrato. Por ello, cualquier decisión que afecte a la conexión, parada, modificación de configuraciones, sustitución, etc. del equipamiento objeto del contrato, debe ser consensuada previamente con los miembros de dicho Área.

Las actualizaciones deberán estar justificadas mediante la emisión de un informe en el que el adjudicatario detalle las causas que motivan la actualización. Una actualización no ocasionará perjuicio sobre el servicio prestado ni sobre los niveles de calidad del mismo. En caso de que fuera necesario interrumpir la prestación de algún servicio o funcionalidad, se acordará con los responsables de sistemas del SIC la fecha y hora de realización de la parada de manera que la incidencia por el corte del servicio sea la mínima posible.

Llegado el caso de que una solución adoptada sin consentimiento del personal del Área de Sistemas del S.I.C. provoque posteriormente mal funcionamiento o interrupciones del servicio, se podrá proceder a una sanción económica proporcional al número de horas de fallo provocadas por dicha anomalía; independientemente de que la resolución del problema se produzca dentro de los plazos establecidos en el acuerdo de nivel de servicio.

11. PLANIFICACIÓN, DIRECCIÓN Y SEGUIMIENTO DEL CONTRATO

Una vez adjudicado el presente concurso y realizados los trámites administrativos necesarios para la formalización del contrato, el adjudicatario se reunirá con el personal de la Universidad de Burgos y se procederá al nombramiento de una comisión de seguimiento del proyecto. Esta comisión estará presidida por el director de proyecto e incorporará personal perteneciente a la UBU y a la empresa adjudicataria.

Corresponde a la **Comisión de seguimiento** la supervisión y dirección de los trabajos, proponer las modificaciones que sea conveniente introducir o, en su caso, proponer la suspensión de los trabajos si existiese causa suficientemente motivada.

Durante la fase de implantación la Comisión de seguimiento se reunirá a petición del responsable del contrato de la UBU y tendrá sus reuniones en las instalaciones de la Universidad de Burgos o por videoconferencia.

Formarán parte de la Comisión de seguimiento:

- El responsable del contrato que será el responsable del proyecto por parte de la

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

UBU
- Personal técnico del Servicio de Informática y Comunicaciones
- El Director del Proyecto por parte de la empresa adjudicataria
- Un técnico responsable del proyecto designado por la empresa adjudicataria

Las funciones de esta Comisión serán las siguientes:

- Seguimiento y evaluación del progreso de las tareas y plazos planificados para la implantación y prestación de los servicios.
- Coordinación de las reuniones e informes de seguimiento del proyecto.
- Verificación del cumplimiento de las especificaciones solicitadas y definición de los requisitos pendientes.
- Negociación para la incorporación de nuevas prestaciones o requisitos.
- Cualquier otro asunto que la propia comisión considere de interés.

Una vez finalizada la implantación, **se mantendrá como mínimo una reunión trimestral** entre el personal del SIC y la empresa adjudicataria. **En las reuniones se revisarán los informes de cumplimiento de los Acuerdos de Nivel de Servicio y el estado de la bolsa de horas.**

Será obligatorio para la empresa adjudicataria elaborar un acta en la que quede constancia de todos los aspectos tratados en cada reunión de la Comisión de Seguimiento.

12. SEGURIDAD DE LA INFORMACIÓN

La configuración de las infraestructuras deberá cumplir las medidas especificadas por el Esquema Nacional de Seguridad para un sistema **de categoría media**.

Los servicios alojados en cloud que estén incluidos en el alcance del contrato deberán estar certificados en la norma ISO/IEC 27017 o equivalente.

El personal asignado por la empresa adjudicataria deberá conocer y respetar la normativa de seguridad de información de la UBU (http://www.ubu.es/normativa/administracion-y-gestion-general-de-la-universidad/seguridad-de-la-informacion), así como los procedimientos establecidos por la Universidad que sean de aplicación en el ámbito del contrato.

Al margen de las auditorías realizadas por el equipo técnico de la UBU o empresas de auditoría contratadas por la Universidad, **la empresa adjudicataria deberá realizar, al menos, una auditoría de hacking ético después de la implantación**. El informe se entregará a la UBU y el adjudicatario deberá aplicar las correcciones necesarias en la

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

configuración de los componentes para solventar las vulnerabilidades detectadas en las auditorías.

Será de obligado cumplimiento para el adjudicatario colaborar con el Servicio de informática y Comunicaciones y aplicar la solución a las vulnerabilidades e incidencias de seguridad que vayan surgiendo.

Se deberán especificar los procedimientos de mantenimiento para proteger el sistema en su conjunto (seguridad en el software empleado, gestión de cambios, gestión de la configuración, gestión de la capacidad, gestión de vulnerabilidades, etc.).

Para la prevención de actualizaciones fallidas, la empresa adjudicataria se asegurará previamente mediante comunicación escrita a los técnicos de la universidad, de la existencia de copias de seguridad convenientemente actualizadas o tomará medidas adicionales como la creación de ficheros o tablas de respaldo para almacenar la información a modificar, con el fin de poder restaurarla en caso de fallo.

13. PROTECCIÓN DE DATOS

La empresa adjudicataria se compromete a tratar los datos de carácter personal en el ámbito del servicio objeto de este pliego, de conformidad con lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y la normativa que la desarrolla.

También se compromete a tratar los citados datos, únicamente conforme a las instrucciones de la Universidad de Burgos y a no aplicarlos o utilizarlos con fin distinto al del servicio objeto de este pliego ni a comunicarlos, ni siquiera para su conservación, a otras personas.

Los sistemas alojados en servicios cloud que estén incluidos en el alcance del contrato deberán estar certificados en la norma ISO/IEC 27018 o equivalente.

14. PROPIEDAD INTELECTUAL Y CONFIDENCIALIDAD

La empresa adjudicataria y cualquier persona dependiente de la misma que desempeñe las funciones objeto de este pliego deberán mantener la confidencialidad plena sobre la información relativa a los servicios objeto del mismo. Esta obligación de confidencialidad se entenderá plenamente vigente incluso con posterioridad a la extinción del servicio prestado.

Todos los informes, estudios y documentos resultantes de este pliego serán propiedad de la UBU, reservándose ésta todas las facultades inherentes a este derecho, pudiendo reproducirlos, publicarlos o divulgarlos parcialmente o en su totalidad, en la medida que tenga conveniente, sin que pueda oponerse por ello la empresa adjudicataria alegando derechos de autor.

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es

El adjudicatario no podrá hacer ningún uso o divulgación de los informes, estudios y documentos elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa por escrito de la UBU.

Los trabajos englobados en este pliego se entenderán como confidenciales, debiendo el adjudicatario asegurar de la forma más razonable posible esta característica.

La Jefa del Servicio de Informática y Comunicaciones

Edificio de Servicios Administrativos, 2ª planta C/ Don Juan de Austria nº 1 09001 Burgos
Tel: 947 25 88 43 e-mail: serv.informatica@ubu.es