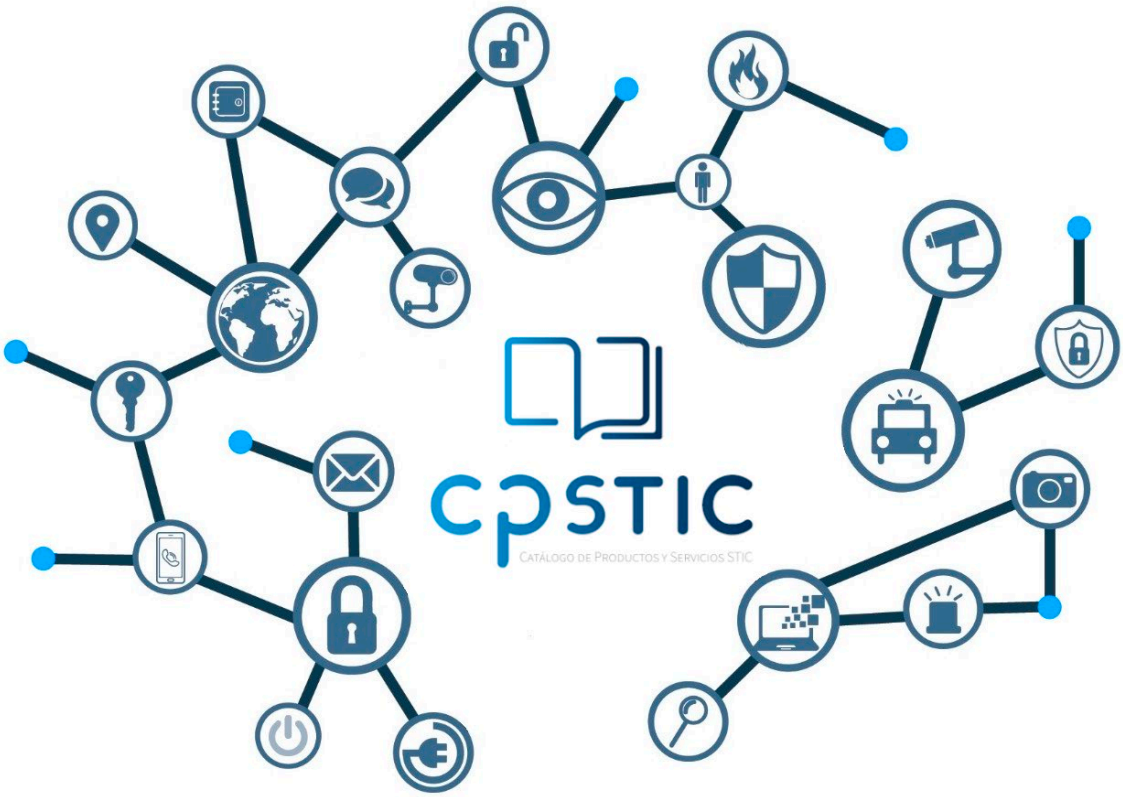
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1616

Procedimiento de Empleo Seguro
PEXIP INFINITY



Abril 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.04.19 17:24:48 +02'00'

NIPO: 083-23-119-6.
Fecha de Edición: abril de 2023.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. **Pexip Infinity es una plataforma de infraestructura de videoconferencia**, totalmente *software*, virtualizada y distribuida para gestionar equipos de videoconferencia de sala H.323/SIP, clientes de escritorio para PC, Mac, Linux con cliente WebRTC, y cliente para dispositivos móviles IOS y Android.
2. Pexip Infinity actúa como:
   - *Call Control*: SIP Register y *Gatekeeper* para terminales H.323/SIP de cualquier fabricante.
   - *Session Border Controller* y *Firewall Traversal*.
   - Unidad de Multiconferencia (MCU) que entre otras funciones incorpora Salas de Reuniones Virtuales (*Virtual Meeting Rooms* - VMR) a las que se pueden conectar terminales de videoconferencia, usuarios registrados e invitados.
   - Sistema de gestión de terminales.
   - *Bridge de interworking* que permite interoperar con usuarios de *Microsoft Teams*, *Google Meet*, *Skype for Business*, *Webex* y *WebRTC*.
   - También permite generar *streams RTMP* y *RTMPS* para funciones de grabación y *streaming*.
3. Se integra *Outlook* y *Google Calendar* para la planificación de sesiones. Permite el uso de SSO, certificados y LDAP para la autenticación de terminales y usuarios y consta de una amplia librería de APIs.
4. Pexip Infinity puede correr en instalaciones privadas del usuario o en infraestructuras de nube públicas dedicadas como Azure, Google Cloud o AWS.
5. Esta arquitectura es escalable y permite la securización de las comunicaciones mediante cifrado extremo a extremo. Permite la privacidad de datos, equipos y usuarios, mediante la encriptación y custodia de los CDR (Call Data Records) y del acceso securizado a la propia administración del sistema.

2. OBJETO Y ALCANCE

6. El objeto del presente documento es facilitar la instalación y configuración segura de los dispositivos de **Pexip Infinity con la versión 25.4 (Build 59565.0.0) de software y la versión 1.6.2 del cliente**, junto con el aseguramiento del entorno en el que se despliega.
7. **El despliegue del producto se deberá realizar siempre en la modalidad On-Premise, de forma local, dado que esta es la modalidad cualificada e incluida en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC).**
8. En algunos aspectos, se mencionará la necesidad de contactar con el fabricante para obtener soporte. El contacto con el fabricante deberá ser establecido a través de los canales seguros previamente acordados, y especificados en la memoria técnica del proyecto, o documento similar.

3. ORGANIZACIÓN DEL DOCUMENTO

9. El documento se organiza en los siguientes apartados de contenido específico:

   a) Apartado **4**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.

   b) Apartado 5. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

   c) Apartado **6**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

   d) *Apartado **7***. En este apartado se incluye un *checklist* para verificar las tareas de configuración segura mencionadas a lo largo del documento.

   e) Apartado **8**. En este apartado se incluye el listado de documentos referenciados a lo largo del documento.

   f) Apartado **9**. Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. *Infinity* es un producto exclusivamente *software*, y los paquetes de instalación deben ser descargados desde el sitio web del fabricante Pexip https://www.pexip.com/. Alternativamente, se suministrarán directamente por el personal de soporte del fabricante.
11. **Se debe comprobar integridad de los paquetes** utilizados en el momento de la instalación, realizando su hash y verificando que coincide con el mostrado en la página de descargas.
12. La imagen para la instalación puede ser descargada también desde el siguiente enlace:

    https://dl.pexip.com/infinity/v25.4/index.html
13. En el mismo repositorio se encuentra un fichero *README.TXT* que contiene los hashes para cada fichero descargable. Se debe verificar la integridad de cada fichero, realizar su hash y comprobar que coinciden.

4.2 ENTORNO DE INSTALACIÓN SEGURO

14. Los componentes del producto son instalables en un entorno de virtualización, como *KVM*, *ESXi* de *VMware*, o similar. El equipamiento utilizado para ejecutar **el entorno de virtualización debe ser protegido** de acuerdo a las políticas de uso seguro de la organización.
15. La funcionalidad es independiente de la localización física o emplazamiento de la infraestructura hardware utilizada para su despliegue. Sin embargo, deben tenerse en cuenta las características de control de tráfico que existan en el entorno, por ejemplo, debe tenerse en cuenta la existencia de elementos firewall o proxy que controlen y bloqueen flujos de tráfico en determinados puertos o protocolos.
16. Deberán proporcionarse las configuraciones necesarias en estos elementos de control para permitir el tráfico entre los nodos. Se pueden consultar los puertos y protocolos utilizados en el siguiente enlace:

    https://docs.pexip.com/admin/port_usage.htm?Highlight=ports

4.3 NODOS OPERACIONALES

17. El despliegue del producto se divide en distintos nodos operacionales que facilitan las distintas funcionalidades:

    a) Nodo de gestión (*Management Node*). Proporciona la interfaz administrativa del producto. Permite a los administradores crear y gestionar el resto de nodos, configurar los servicios, ver las estadísticas y gestionar los participantes de las conferencias.

    b) Nodo de conferencia (*Conferencing Node*). Proporcionan las funcionalidades de conferencia. Ejecutan los servicios configurados en los nodos de gestión. Pueden adoptar los siguientes roles:

    - *Transcoding role*: permite al nodo gestionar y albergar conferencias.

- *Proxying role*: permite al nodo reenviar la información a nodos con rol *Transcoding*.

4.4 REGISTRO Y LICENCIAS

18. Para emplear todas las funcionalidades del producto, deben instalarse las correspondientes licencias. El procedimiento de instalación de licencias puede ser llevado a cabo *online* u *offline*. El procedimiento *online* requiere de comunicación directa entre el nodo de gestión y los servidores de licenciamiento habilitados por el fabricante en Internet, por lo que debería habilitarse dicha comunicación.
19. En una instalación segura, se considerará preferible el aislamiento completo del nodo gestor, por lo que no podría comunicarse con servidores externos. En estas situaciones, debe considerarse el procedimiento de activación *offline*, descrito en el siguiente enlace:

    https://docs.pexip.com/admin/licenses.htm#Manually
20. Para el acceso a esta utilidad, se debe contactar con el soporte del fabricante.
21. El detalle de instalación de las licencias se puede consultar en el apartado *Pexip Infinity license installation and usage* de la guía *Pexip Infinity Aministrator Guide – REF1*.

4.5 CONSIDERACIONES PREVIAS

22. El entorno de virtualización que se utilizará para la ejecución de las máquinas virtuales que componen el sistema *Infinity* debe ser securizado de acuerdo a las instrucciones proporcionadas por el suministrador del mismo.
23. Se soportan los siguientes hipervisores:
    - *Vmware vsphere ESXi* (recomendado mínimo *vSphere Standard Edition*).
    - *Microsoft Hyper-V.*
    - *KVM.*
    - *Xen.*
24. Otros hipervisores pueden ser utilizados, aunque pueden aplicarse limitaciones específicas. **Se requiere siempre de direccionamiento IP estático** para las máquinas virtuales de *Infinity.*
25. En el caso específico de *vmware ESXi*, se deben seguir las indicaciones de la guía *Security Technical Implementation Guide*, accesible desde el siguiente enlace. En el resto de casos, se deberá seguir la guía equivalente correspondiente al sistema de virtualización empleado.
26. En el servidor utilizado para el entorno de virtualización se debe considerar la utilización de al menos dos (2) interfaces físicos de red (NICs) que permita la separación entre el acceso a la gestión del propio entorno de virtualización y a las máquinas virtuales del sistema *Infinity*.
27. Deben reservarse los recursos necesarios para la ejecución de las máquinas virtuales (CPU, memoria, disco) de manera que cada una de las máquinas obtenga los recursos necesarios para la ejecución de sus tareas sin interferencia de otras máquinas virtuales en el mismo servidor. Para ello, además de proceder a la fijación de los recursos tras la instalación, **el**

administrador del sistema debe comprobar previamente que en el servidor existe la capacidad suficiente.

28. Las máquinas virtuales facilitadas para la instalación (nodos de gestión y conferencia) incluyen todo el *software* necesario para el funcionamiento del producto, por lo que no se deberá instalar ningún software adicional.

4.6 INSTALACIÓN

29. La primera tarea consiste en la instalación del nodo de gestión. Una vez descargado el software, tal como se indica en el apartado 4.1 ENTREGA SEGURA DEL PRODUCTO, se seguirán las instrucciones correspondientes para la instalación en el entorno de virtualización utilizado. En el siguiente enlace se pueden consultar los pasos necesarios para cada entorno de virtualización:

    https://docs.pexip.com/admin/installation_overview.htm

30. Debe procederse a **la securización de la BIOS de cada máquina virtual** para asegurarse de que el arranque se efectúa en condiciones controladas y del dispositivo correcto sin interferencias. Por ejemplo, mediante la configuración de una contraseña para el acceso a la BIOS.

31. La primera ejecución del sistema, en el momento del arranque de la máquina virtual, pedirá la introducción de los datos de configuración (*installation wizard*) Deben configurarse el usuario y contraseña para acceder al sistema posteriormente, tanto por el interfaz tipo intérprete de comandos (*bash*) como por interfaz gráfico web. No existen contraseñas por defecto. **Dicha contraseña deberá cumplir con lo indicado en el apartado 5.4.4 POLÍTICA DE CONTRASEÑAS.**

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

32. El producto permite la configuración de un modo de operación seguro, pero este no se encuentra configurado por defecto. Por lo tanto, **se deberá configurar el producto para funcionar en este modo**.

33. Para ello, una vez instalado el nodo de gestión, se deberá ejecutar en el interfaz de gestión el comando *securitywizard*. Dicho comando es accesible como un script de *Shell*, por lo que para su ejecución será necesario acceder al nodo de gestión por consola o de forma remota por SSH (si no está deshabilitado previamente).

34. Tras su ejecución, el producto realizará una serie de preguntas, en las cuales **se deberán modificar los siguientes valores por defecto**:

    - *Enable FIPS 140-2 compliance mode*. Introducir el valor *YES*. Activa el modo de empleo seguro.
    - *Disable system administrator account (this applies to SSH and console access).* Introducir el valor YES. Impide el acceso a nivel de Sistema Operativo.
    - *Accept ICMPv6 redirects*. Introducir el valor *NO*. Impide las redirecciones de tipo ICMPv6.
    - *Drop incoming packets to closed ports rather than reject*. Introducir el valor *YES*. Descarta los paquetes recibidos en puertos cerrados en lugar de rechazarlos.
    - *Accept multicast ICMPv6 echo requests*. Introducir el valor *NO*. Deniega los paquetes de tipo *ICMPv6 echo*.
    - *Enable IPv6 Duplicate Address* Detection. Introducir el valor *NO*.
    - *Active management web sessions*. Introducir un valor de 100. Configura un máximo de 100 sesiones de administrador imultaneas.
    - *Active per-user management web* sessions. Introducir un valor de 10. Limita el número de sesiones simultaneas por usuario a 10.
    - *Enable TLS < 1.2*. Introducir el valor *NO*. Impide el uso de versiones de TLS inferiores a 1.2.
    - *Enable Anonymous DH for outbound SIP/TLS*. Introducir el valor *NO*. Impide el uso de Diffie-Hellman anónimo en conexiones salientes.
    - *Permit TLS <1.2 for inbound HTTPS*. Introducir el valor *NO.* Impide el uso de versiones de TLS inferiores a 1.2 en conexiones HTTPS entrantes.
    - *Enable FIR*. Introducir el valor *YES.* Solicita el refresco de vídeo de imagen completa en el protocolo *Full Intra Request*.
    - *Enable AES128-SHA ciphersuite*. Introducir el valor *NO*. Deshabilita el uso de las ciphersuites con AES128-SHA.
    - *Enable AES128-SHA ciphersuite for outbound SIP/TLS*. Introducir el valor *NO*. Deshabilita el uso de las ciphersuites con AES128-SHA en conexiones salientes.

35. Una vez finalizado este proceso, el sistema se reiniciará.

5.2 AUTENTICACIÓN

36. El producto requiere la autenticación de los administradores para el acceso a la gestión y configuración, mediante los siguientes métodos:

    - Credenciales locales, mediante usuario y contraseña o certificados, almacenadas en el propio sistema. Para la creación y gestión de usuarios locales, ver apartado 5.4.2 CONFIGURACIÓN DE ADMINISTRADORES.
    - Servidores de autenticación externos. Mediante la integración con servidores de tipo *LDAP*. Ver apartado 5.3 SERVIDORES DE AUTENTICACIÓN. **Se recomienda emplear este método para la autenticación de administradores**.

37. En caso de emplear certificados para la autenticación, se debe configurar el parámetro *Require client certificate* desde *Users & Devices > Administrator Authentication*. Se pueden seleccionar los siguientes valores:

    - *Not required*. No se solicitarán certificados en el proceso de autenticación.
    - *Required (user identity in subject CN).* Para acceder se deberá presentar un certificado cuyo CN coincida con el configurado para dicho usuario.
    - *Required (user identity in subjectAltName userPrincipalName).* Para acceder se deberá presentar un certificado cuyo *subjectAltName userPrincipalName* coincida con el configurado para dicho usuario.

38. Adicionalmente, permite la integración con un servidor de *Active Directory*, para la autenticación de los clientes para acceder a las funcionalidades de videoconferencia. **Se debe configurar dicha integración**. Para ello, consultar el siguiente enlace.

5.3 SERVIDORES DE AUTENTICACIÓN

39. El detalle de configuración de los servidores de autenticación externos se puede consultar en el siguiente enlace: https://docs.pexip.com/v25/admin/integrate_ldap.htm

40. **Se recomienda que la cuenta utilizada para el acceso al servidor de directorio no tenga privilegios de escritura**, por lo que se recomienda utilizar una “cuenta de servicio” y no la del administrador.

41. **Se deberá emplear el mecanismo de LDAPv3 basado en START-TLS sobre el puerto TCP 389**. En caso de que el servidor LDAP utilice certificados emitidos por una autoridad no reconocida, es necesario instalar los certificados de dicha CA en el producto, para ello ver apartado 5.7 GESTIÓN DE CERTIFICADOS.

42. Para un empleo seguro de LDAP, desde *Users & Devices > Administrator Authentication*. Se debe accede a *LDAP Configuration* y asegurar que la casilla *Allow insecure transport* no se encuentra seleccionada. De esta forma **se exigirá el empleo de TLS en las conexiones con LDAP.**

5.4 ADMINISTRACIÓN DEL PRODUCTO

5.4.1 ADMINISTRACIÓN LOCAL Y REMOTA

43. El producto dispone de las siguientes interfaces para la administración:

- Acceso local de tipo *Shell bash*, mediante SSHv2 por defecto. Se empleará esta interfaz para la configuración del modo de empleo seguro, tras lo cual quedará deshabilitada (ver apartado 5.1 MODO DE OPERACIÓN SEGURO).
- Administración remota de tipo GUI mediante HTTPS. **Se recomienda configurar y gestionar el producto haciendo uso de esta interfaz**. Se deberán configurar los certificados de servidor para el correcto funcionamiento, ver apartado 5.7 GESTIÓN DE CERTIFICADOS.

44. **No se debe realizar el acceso al sistema empleando otros protocolos**. Los servicios correspondientes se encuentran deshabilitados por defecto.
45. Para verificar que se ha deshabilitado la gestión mediante SSH, ir a *Platform > Global settings > Connectivity* y verificar que la casilla *Enable SSH Setting* se encuentra con el valor *off*.

5.4.2 CONFIGURACIÓN DE ADMINISTRADORES

46. Durante el proceso de instalación se genera un usuario administrador con todos los privilegios (ver apartado 4.6 INSTALACIÓN).
47. El usuario de administración dispone de privilegios para configurar el sistema a través del interfaz de gestión. Con el fin de aumentar la seguridad se configurará la autenticación y autorización de los usuarios privilegiados mediante un servidor LDAP centralizado, tal como se ha visto en el apartado 5.3 SERVIDORES DE AUTENTICACIÓN. Una vez configurado el servidor externo, se debe configurar el producto para emplearlo, para ello ir a *Users & Devices > Administrator Authentication* y configurar el parámetro *Authentication source* con el valor *LDAP database and local database.*
48. De esta forma, en caso de perder conexión con el servidor externo, será posible acceder consultando la base de datos local. Si no, en caso de pérdida de conexión sería imposible realizar el acceso.
49. Es posible configurar los roles de administración según las necesidades de la organización. Para ello, dede *Users & Devices > Administrator Roles*, se pueden seleccionar roles existentes y modificar sus permisos, o generar roles nuevos.
50. El detalle de configuración de los roles de usuario se puede consultar en el siguiente enlace.

5.4.3 PARÁMETROS DE SESIÓN

51. **Se deberán configurar los parámetros de sesión**. Para ello, ir a *Platform > Global System Settings* y configurar los siguientes parámetros:
    - *Login banner text.* Configura un mensaje de aviso y consentimiento en el inicio de sesión (*banner*). Este se presentará antes de la autenticación de los usuarios.
    - *Management web interface session timeout*. Configura el tiempo de inactividad, tras el cual se desconectará a un usuario. Se deberá configurar un valor de cinco (5) minutos.

5.4.4 POLÍTICA DE CONTRASEÑAS

52. Se deberá configurar/exigir la siguiente política de contraseñas en el servidor de autenticación externo o de forma procedural:

    - Longitud mínima de **doce (12) caracteres**.
    - Emplear, al menos, **una letra minúscula, una mayúscula, un número y un carácter especial.**
    - **No reutilizar** las últimas cinco (5) contraseñas.
    - Cambiar las contraseñas **cada sesenta (60) días.**
    - No permitir un nuevo cambio de contraseñas **antes de pasados 10 días**.

5.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

53. Las máquinas virtuales disponen de una configuración por defecto que solamente permite el uso de los protocolos y servicios estrictamente necesarios para el uso del producto. Dicha configuración es gestionada automáticamente por el sistema que la monitoriza continuamente, y no está soportada la manipulación de la misma por el usuario.
54. La configuración del *firewall iptables* que se suministra con el producto bloquea por defecto la comunicación en todos los puertos no empleados. **Solo se podrá modificar la configuración de *iptables* en caso de ser estrictamente necesario, de forma general no deberá modificarse**.
55. El producto no admite el empleo de *proxies*, inspección de tráfico o mecanismos similares, que serán detectados como ataques de tipo “Man In the Middle”.
56. Deberá asegurarse que los siguientes parámetros se encuentran deshabilitados desde *Platform > Global Settings*:

    - *Enable Http Access for external systems.*
    - *Enable SSH.*

5.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

57. Tal como se ha visto, durante la activación del modo de empleo seguro (ver apartado 5.1 MODO DE OPERACIÓN SEGURO), no se permite el uso de versiones de TLS anteriores a 1.2.
58. La versión de SSH utilizada por el producto es SSHv2 por defecto y no requiere de configuración adicional.
59. El producto emplea el protocolo IPsec para la comunicación segura entre los nodos del sistema. En el momento de la inicialización del nodo de gestión, se generan las claves privada y pública correspondientes. No es posible alterar la configuración de las conexiones IPsec. Para la comunicación entre los nodos es necesario permitir en los *firewalls* de la organización el tráfico de:

    - IP Protocol 50 (ESP).
    - TCP/UDP Port 500 (IKE).

60. El protocolo IPsec emplea los siguientes parámetros no configurables para el canal inicial para intercambio de claves (ISAKMP) y los túneles ESP:
    - Cifrado con el algoritmo 256-bit AES-GCM.
    - Intercambio de claves con 4096 DH.
61. La comunicación con IPsec se establece entre el nodo manager y los nodos de conferencia y los nodos de conferencia entre sí. Los nodos que pertenecen a una "*location*" sólo requieren de comunicación entre sí y con el nodo manager.
62. Cuando se registren equipos de videoconferencia en el sistema, será obligatorio el uso de TLS como transporte seguro de la señalización y se habilitará el cifrado del tráfico de media, SRTP para SIP y H.235 para *endpoints* H.323. Para ello, se deberá:
    - Habilitar el parámetro *SIP-TLS certificate verification mode* con el valor *Required* en la configuración desde Global Settings -> Security.
    - Habilitar el parámetro *Media Encryption* con el valor *Required* en la configuración de *Global Settings -> Connectivity.*

5.6.1 PROTOCOLOS EXTERNOS AL PRODUCTO

63. Para todos los protocolos seguros, como SIP sobre TLS o SRTP debe tenerse en cuenta que los algoritmos y funciones criptográficas que se utilicen, deben estar admitidos según la guía CCN-STIC-807. En este aspecto, hay que considerar que es un proceso en el que participan elementos externos al producto. Por ejemplo, la negociación entre los extremos de una sesión SDP establece el intercambio de las funciones y algoritmos criptográficos utilizados durante la misma. Por ello, debe prestarse atención a que los usuarios del sistema deben tener la posibilidad de utilizar los mismos mecanismos. El usuario del sistema que accede a una conferencia utilizando un navegador, o un cliente SIP, debe tener la posibilidad de negociar los parámetros de cifra de la sesión al nivel requerido. Esta negociación es por sesión.
64. Para todos los protocolos que utilice el producto y sean configurados en un sistema externo, debe tenerse en cuenta que los algoritmos y funciones criptográficas que se utilicen, deben estar admitidos según la guía CCN-STIC-807. **DSA o RSA con claves de, al menos, 3072 bits de longitud.**
    - **ECDSA con curvas P-256 o superior.**
    - **Funciones Hash SHA-256 o superior.**
    - **Cifrado AES-128 o superior.**
    - **Grupos *Diffie-Hellman* 15, 16, 19, 20, 21, 28, 29 o 30.**
    - ***Elliptic Curve Diffie-Hellman* P-256 o superior.**
65. Los clientes web usarán HTTPS TLS para la señalización y DTLS-SRTP para media.

5.7 GESTIÓN DE CERTIFICADOS

66. En el momento de la instalación del sistema, por defecto se generan certificados autofirmados. **Estos deberán sustituirse por certificados firmados por una CA de confianza.**

67. Deberán seguirse los siguientes pasos generales:
    - Importar el certificado de la CA que se utilizará para generar el certificado de servidor.
    - Crear un CSR (*Certificate Signing Request*). Se deberá utilizar uno de los siguientes parámetros para la creación del certificado:
        - **Tipo de clave ECDSA, con un tamaño de 256 o 384 bits y algoritmo de firma SHA-384 o SHA-256.**
        - **Tipo de clave RSA, con una longitud de clave de 3072 bits o superior.**
    - Importar el certificado de servidor una vez recibido, para todos los nodos. Este se empleará para todas las conexiones mediante TLS. El formato admitido para la importación es un fichero .cer conteniendo X509 codificado Base64.
    - Si se desea, se puede generar un certificado único para cada nodo, seleccionando el nodo específico que lo empleará al importar el certificado.
68. El proceso de generación de una solicitud de firma de certificado (*Certificate Signing Request - CSR*) se puede consultar en el siguiente enlace:

    https://docs.pexip.com/admin/certificate_signing_request.htm
69. En ocasiones podría no disponerse de la opción de generar el CRL en la interfaz de gestión. En dicho caso, es posible generar los certificados (siempre cumpliendo las condiciones indicadas anteriormente) empleando el comando *openssl*, mediante la consola del producto o un sistema externo, para importarlo posteriormente. En caso de emplear un sistema externo, asegurarse de conservar las claves privadas empleadas para la generación. Se puede consultar el siguiente enlace para ver las opciones del comando.
70. El detalle de configuración de los certificados TLS y CAs del producto se puede consultar en el siguiente enlace:

    https://docs.pexip.com/admin/certificate_management.htm
71. Se recomienda también activar la verificación OCSP en las conexiones SIP TLS con usuarios. Para ello es necesario configurar la opción *SIP TLS Verification mode* a *On*. El detalle de configuración de esta opción se puede consultar en el siguiente enlace:

    https://docs.pexip.com/admin/verify_tls.htm

5.8 SINCRONIZACIÓN HORARIA

72. Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados para permitir una alta fiabilidad en los sistemas de auditoría y *logging*.
73. El producto permite configurar la sincronización con servidores de tiempo mediante NTP. Para ello seguir los siguientes pasos:
    - Ir a *System > NTP Servers.*
    - Introducir los datos del servidor de tiempo.
    - **Se deberá hacer uso de autenticación NTP**, para ello incluir un ID de clave, así como la clave. Solo se encuentra disponible el uso de claves SHA1.

- Repetir los pasos anteriores por cada servidor que se desee incluir. Se recomienda hacer uso de tres orígenes de tiempo distintos.

5.9 ACTUALIZACIONES

74. Para la actualización del sistema se dispone de un espacio desde el que descargar los paquetes de actualización en el sitio web de Pexip: h*ttps://dl.pexip.com*

75. Después de proceder a la descarga del paquete de actualización, es necesario comprobar su autenticidad y no manipulación. Para ello, **se deberá realizar el hash sha256 del fichero descargado** y verificar que coincide con el mostrado en la página de descarga o en el fichero "README.TXT" del apartado de descargas.

76. El detalle sobre cómo llevar a cabo las actualizaciones del producto se puede consultar en el siguiente enlace: *https://docs.pexip.com/admin/upgrading.htm*

5.10 AUTO-CHEQUEOS

77. El sistema dispone de monitorización completa de ficheros de configuración de las funciones críticas que restablece la configuración almacenada en caso de detectar modificaciones no autorizadas de las mismas.

78. El sistema de monitorización opera tanto en el arranque inicial como a intervalos periódicos establecidos para dicha comprobación.

79. En caso de la detección de alguna inconsistencia, se presentará una alarma y se restaurará la configuración a la última registrada.

80. En caso de que no sea posible la restauración al haberse producido un fallo catastrófico irrecuperable, el sistema no puede continuar en servicio y será necesaria la restauración desde una copia de *backup*.

5.11 SNMP

81. El producto soporta SNMP para propósito de monitorización del sistema únicamente, y no para el servicio. SNMP se considera en general un protocolo inseguro y únicamente SNMPv3 provee mecanismos de cifrado entre el equipo y el servidor de gestión y autenticación mediante usuario/contraseña. Por tanto, **se debe utilizar únicamente SNMPv3 en caso de ser necesario.**

82. El detalle de configuración se SNMP se puede consultar en el siguiente enlace: https://docs.pexip.com/admin/enabling_snmp.htm

83. Para habilitar sólo SNMPv3, se deberá seleccionar el modo *SNMPv3 read-only*. Una vez seleccionado se deberán configurar los parámetros: *SNMPv3 Privacy Password*, *SNMPv3 username* y *SNMPv3 authentication password.*

5.12 ALTA DISPONIBILIDAD

84. El sistema *Infinity* no dispone de una configuración específica de alta disponibilidad. Sin embargo, provee mecanismos integrados de alta disponibilidad del servicio, que se apoyan en las siguientes características:

- En caso de fallo temporal del nodo de gestión, los nodos de conferencia seguirán funcionando con la configuración establecida de forma indefinida hasta que se restaure una copia de seguridad del nodo de gestión. Si la restauración se efectúa desde una copia que incluya la configuración, el sistema continúa prestando servicio sin interrupción.
- Si la recuperación del nodo de gestión requiere de la regeneración del sistema desde su modo de inicio, será necesario recuperar los nodos de conferencia, ya que no coincidirán las claves criptográficas almacenadas.
- Se recomienda desplegar varios nodos de conferencia en cada *location* y repartir las conexiones entre ellos a través de un mecanismo externo (por ejemplo, mediante *DNS load balancing*).
- En el caso de los nodos *proxy-edge* puede utilizarse igualmente un mecanismo de reparto por DNS, y se soportan balanceadores/*proxies* externos del tipo reverse proxy (como, por ejemplo, NGINX y similares).

5.13 AUDITORÍA

5.13.1 REGISTRO DE EVENTOS

85. El producto realiza la generación de eventos de auditoría relevantes. Los registros se rotan en ficheros de 10 Mbytes y se conservan hasta alcanzar 2Gbytes. Una vez alcanzado dicho umbral, el producto comenzará a sobrescribir los registros más antiguos automáticamente. En caso de llenado del sistema de ficheros, se genera una alarma.
86. Adicionalmente el administrador del sistema puede realizar el borrado de los ficheros necesarios para liberar espacio. El borrado manual puede efectuarse:
    a) En el interfaz de gestión cli, acceder al directorio */var/log.*
    b) Borrar los ficheros con sufijo numérico (*fichero.X*) que sean necesarios con el comando *rm fichero.X*.
87. En el siguiente enlace se puede consultar el detalle de los distintos eventos generados, así como la información que contienen:

    https://docs.pexip.com/api_manage/logs.htm
88. El administrador puede acceder a un subconjunto de los eventos filtrados, llamado *Administrator log*, que contiene la información sobre los eventos de seguridad (cambios de configuración, copias de seguridad, etc). La descripción de los módulos en este subconjunto puede verse en:

    https://docs.pexip.com/api_manage/logs.htm#modules
89. **Se recomienda configurar el envío de los registros a un servidor syslog externo**. La conexión entre el nodo de gestión y el servidor se establecerá mediante protocolo TLS v1.2. Para ello, seguir los siguientes pasos:
    - Ir a *System > Syslog Servers*.
    - Introducir los datos del servidor al que se desea enviar los registros.
    - Seleccionar *TLS* en la casilla *Transport.*

- Seleccionar el envío de *Support logs, Audit Logs* y *Web Server Logs*.

90. El detalle de configuración del envío de registros a servidores externos se puede consultar en el siguiente enlace:

    https://docs.pexip.com/admin/enabling_syslog.htm

91. Se deberá tener en cuenta que cada nodo envía sus propios registros al servidor remoto, con origen su dirección IP.

5.14 COPIAS DE SEGURIDAD

92. Las copias de seguridad del sistema pueden incluir las características de configuración en el sistema, y la propia máquina virtual del nodo de gestión. **Se recomienda mantener copias de seguridad periódicas de ambos**.

93. El producto dispone de dos (2) formas de realizar copias de los datos de configuración:

    - Emplear los mecanismos del hipervisor para realizar una copia o *snapshot* del nodo de gestión. Las copias o *snapshot* creadas, deberán almacenarse de forma segura.
    - Emplear el mecanismo de copia y restauración incluido en la interfaz de administración del producto.

94. Para crear una copia de forma manual, ir a *Utilities > Backup/Restore*, en la sección *Create backup* introducir una contraseña en los campos *Passphrase* y *Re-enter passphrase*, esta será empleada para proteger la copia. Finalmente pulsar sobre *Create backup*. El producto permite descargar las copias para almacenarlas fuera de la máquina virtual. Para ello, hacer clic en *Download backup*. Estos deberán almacenarse de forma segura.

95. Para habilitar la funcionalidad de copias de seguridad programadas, ir a *Utilities > Automatic Backups*, seleccionar *Enable automatic backups* e introducir una contraseña. Las copias se llevarán a cabo cada día a las 01.02 UTC, la periodicidad no es configurable. Finalmente, se pueden enviar de forma automática las copias a un servidor externo, especificando en el campo *Upload URL* el servidor deseado. **Para el envío de copias a un servidor, se deberá emplear siempre el protocolo SFTP**, quedando prohibido el uso de FTP.

96. De forma genérica no es necesario efectuar copias de seguridad de los nodos de conferencia, ya que son regenerables a partir del nodo de gestión. En caso de ser necesario, podrían realizarse copias de los mismos empleando las herramientas de *backup* de los hipervisores.

97. El detalle de configuración de las copias de seguridad se puede consultar en el siguiente enlace:

    https://docs.pexip.com/admin/backup_restore.htm?Highlight=backup

5.15 SERVICIOS DE SEGURIDAD

98. El acceso a conferencias virtuales se deberá proteger mediante el uso de un PIN (*Personal Identification Number*) y el uso de la facilidad de "Bloqueo" de conferencia. El PIN puede ser asignado para participantes de tipo Organizador (*host*) o de tipo Invitado (*guest*). Deberá constar de, al menos, seis (6) números.

99. Todos los participantes de una conferencia que usen el PIN de Organizador disponen de los mismos privilegios. Lo que usen el PIN de Invitado no disponen de privilegios de control sobre la conferencia.

100. Se pueden configurar dos (2) tipos de conferencia segura:

- Conferencias con PIN para participantes de tipo Organizador. En estas conferencias, los usuarios de tipo Organizador introducen un PIN. Si no disponen del PIN, se unen por defecto como Invitados.
- Conferencias con PIN diferenciado para participantes de tipo Organizador e Invitado. En estas conferencias, todos los participantes deben introducir un PIN para ser aceptados, bien como Organizadores o como Invitados.

101. Si una conferencia se configura como *locked* los participantes Invitados no podrán unirse a la misma hasta que al menos un Organizador se una.

102. EL detalle de configuración de la funcionalidad PIN para conferencias se puede consultar en el siguiente enlace:

About PINs, Hosts and Guests | Pexip Infinity Docs

103. Para **mitigar los posibles ataques de fuerza bruta sobre las conferencias**, se ofrecen dos características integradas que deben ser configuradas una vez instalado el sistema

- Resistencia a ataques de fuerza bruta sobre PIN. Cuando se habilita este servicio, el sistema bloquea de forma temporal el acceso a una *Virtual Meeting Room* que reciba un excesivo número de intentos de introducción de PIN. Se bloquea cualquier intento de acceso durante 10 minutos si se hace más de 20 intentos en una ventana de 10 minutos. El número de intentos es configurable. Además, se genera una alarma en el sistema. Esta configuración es a nivel de sistema o a nivel de *location*. Se puede consultar cómo configurar la funcionalidad en el siguiente enlace:

  https://docs.pexip.com/admin/breakin_resistance.htm

- Protección contra VoIP Scanner. Cuando se habilita este servicio, el sistema bloqueará el acceso al servicio desde cualquier dirección IP que intente un número excesivo de veces en una ventana de tiempo hacer uso de alguno de los servicios. El acceso se bloquea totalmente para la dirección IP si se intenta más de 20 veces en una ventana de 10 minutos, y se genera una alarma. Se puede consultar cómo configurar la funcionalidad en el siguiente enlace:

  https://docs.pexip.com/admin/breakin_resistance.htm#voip

104. En ambos casos, es posible configurar una lista de direcciones IP que se excluyan de estas medidas de protección (lista blanca) La configuración se efectúa de la manera descrita en:

https://docs.pexip.com/admin/breakin_resistance.htm#allow

105. Adicionalmente, se deberán cifrar las máquinas en las cuales se desplieguen los nodos.

6. FASE DE OPERACIÓN

106. El correcto funcionamiento del producto requiere de unas características que deben estar presentes en el entorno operacional:

- El producto debe contar con las **últimas actualizaciones de seguridad** para preservar al mismo de amenazas y vulnerabilidades conocidas.
- Se deben **mantener y analizar los registros de auditoría**. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
- Se deben **gestionar correctamente los certificados** utilizados, actualizándolos cuando sea necesario, por ejemplo, al expirar.
- Se deben **realizar copias de seguridad** de manera periódica.
- Se deben **realizar comprobaciones del consumo** de memoria RAM y espacio de almacenamiento no volátil (HDD) de las máquinas virtuales.
- Si se detecta la necesidad de aumentar los recursos asignados a las máquinas virtuales, es posible. Se debe tener en cuenta que el aumento solo será efectivo tras reiniciar la máquina virtual afectada.

107. Deben comprobarse con regularidad y periodicidad suficiente los avisos y recomendaciones del fabricante en cuanto a la seguridad del sistema. Pexip publica el correspondiente boletín de seguridad del producto Infinity en el siguiente enlace:

https://docs.pexip.com/admin/security_bulletins.htm

7. *CHECKLIST*

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la integridad de la descarga	☐	☐	
Registro de licencias	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Activación del modo seguro	☐	☐	
SERVIDORES DE AUTENTICACIÓN			
Configuración del servidor LDAP	☐	☐	
ADMINISTRACIÓN DEL PRODUCTO			
Configuración de usuarios	☐	☐	
Configuración de los parámetros de sesión	☐	☐	
CONFIGURACIÓN DE PROTOCOLOS SEGUROS			
Configuración de TLSv1.2 en las conferencias	☐	☐	
GESTIÓN DE CERTIFICADOS			
Importar CA, crear CSR e importar el certificado de servidor	☐	☐	
SINCORNIZACIÓN			
Configuración de un servidor de hora NTP	☐	☐	
COPIAS DE SEGURIDAD			
Creación de los backups	☐	☐	
AUDITORÍA			
Configuración del envío de los logs a un servidor Syslog	☐	☐	

8. REFERENCIAS

108. El enlace principal de soporte de Pexip contiene acceso a toda la documentación técnica y guías del producto online: https://docs.pexip.com/

REF1 *Pexip Infinity Aministrator Guide*
https://docs.pexip.com/files/v25/Pexip_Infinity_Administrator_Guide_v25.b.pdf

REF2 RFC Soportadas
https://docs.pexip.com/admin/supported_rfcs.htm

REF3 Boletines de Seguridad
https://docs.pexip.com/admin/security_bulletins.htm

CCN-STIC-807 CCN-STIC-807 Criptología de empleo en el ENS
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html

9. ABREVIATURAS

API	*Application Program Interface*
BFCP	*Binary Floor Control Protocol*
ENS	Esquema Nacional de Seguridad.
FIPS	*Federal Information Processing Standard*
HSTS	*HTTP Strict Transport Security*
HTTPS	*HyperText Transfer Protocol Secure*
IKE	*Internet Key Exchange*
ISAKMP	*IP Security Association and Key Manage Protocol*
OCSP	*Online Certificate Status Protocol*
PIN	*Personal Identification Number*
RTMP/RTMPS	*Real Time Multimedia Protocol/Secure*
SIP	*Session Initiation Protocol*
SNMP	*Simple Network Management Protocol*
SSO	*Single Sign-On*
TLS	*Transport Layer Security*
VMR	*Virtual Meeting Room*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL