centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1305

Procedimiento de Empleo Seguro
Plataforma Ágata

Septiembre 2022

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

CCN 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
2022.09.09 10:18:25 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-223-9

Fecha de Edición: septiembre 2022

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. ÁGATA es una plataforma de gestión multisistema que ayuda con la prevención de incidencias, respuestas automáticas, recogida de datos (cuadro de mandos), gestión portuaria centralizada, ejecución de acciones directamente sobre los activos monitorizados; además de aportar una mayor eficiencia y visibilidad sobre la administración TIC del negocio.

2. OBJETO Y ALCANCE

2. El objeto del presente documento es facilitar la instalación y configuración segura de los dispositivos **Ágata con la versión de software 2.3.3**, junto con el aseguramiento del entorno en el que se despliega.
3. **Este producto ha sido cualificado e incluido en el Catálogo de Productos y Servicios STIC (CPSTIC), en la categoría "Seguridad OT".**

3. ORGANIZACIÓN DEL DOCUMENTO

4. El documento está estructurado en los siguientes apartados:
    a) Apartado **4**. Fase de despliegue en instalación.
    b) Apartado **5**. Recomendaciones en la fase de configuración y administración.
    c) Apartado **6**. Recomendaciones en la fase de operación.
    d) Apartado **7**. *Checklist* de las tareas a realizar y el estado de cada una de ellas.
    e) Apartado **8**. Referencias usadas en este documento.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

5. La entrega del producto se puede llevar a cabo de una de las siguientes formas, en función del tipo adquirido:
    a) Mediante un servidor con el *software* preinstalado, si la organización así lo ha contratado. En este caso, se deberá verificar que el embalaje de entrega no presenta signos de haber sido manipulado.
    b) Mediante la entrega de un enlace seguro para realizar la descarga de la ISO de instalación y otro para los artefactos a desplegar. En este caso, se debe solicitar al fabricante un valor hash para verificar la autenticidad del software descargado.

4.2 ENTORNO DE INSTALACIÓN SEGURO

6. La plataforma Ágata está pensada para su despliegue seguro en el Centro de Procesamiento de Datos (CPD) de la organización, con acceso físico restringido y limitado a un conjunto de personas que posean autorización expresa.
7. Únicamente será accesible desde el puerto 443 para visualizar el frontal de la plataforma, y el puerto 22 para el acceso SSH mediante credenciales para su mantenimiento dentro de la red.

4.3 REGISTRO Y LICENCIAS

8. La plataforma Ágata se usa bajo licencia directa, esto es, no es necesaria validación de licencia ya que su uso se licencia bajo pedido previo. El acceso a los descargables está protegido mediante el uso de los certificados de la organización.

4.4 CONSIDERACIONES PREVIAS

9. Tal y como indica el *Manual de Despliegue – REF1*, durante la instalación se generarán los certificados de comunicación entre los componentes de monitorización de la plataforma. **Se recomienda modificar dichos certificados por unos generados por la CA de confianza de la organización, tal como se indica en el apartado 5.5 GESTIÓN DE CERTIFICADOS**.
10. Por norma general y, dada la naturaleza de la herramienta, en este caso particular, todas aquellas claves y certificados generados en el proceso de instalación indicado en la guía *Instrucciones de Despliegue Ágata Standalone – REF1* deben guardarse en repositorios seguros, protegidos contra accesos o modificaciones no autorizadas.
11. En caso de adquirir únicamente el *software* del producto, los requisitos mínimos para poder operar la herramienta correctamente son los siguientes:
    a) *Hypervisor VMWare ESXI/ESX* 4.0 o superior.

b) Sistema Operativo: Debian 11 64 bits

c) Requisitos mínimos de CPU: 10 vCPU's

d) Memoria RAM no compartida: 40GB

e) Disco Duro 1: 50 Gigas para el sistema y partición de swap

f) Disco Duro 2: 250 Gigas mínimos para datos en PRODUCCIÓN y 100GB para PRE.

Nota: El hipervisor y el sistema operativo utilizados deben tener soporte de seguridad de fabricante y estar parcheados.

4.5 INSTALACIÓN

12. El detalle sobre los pasos necesarios para llevar a cabo la instalación se puede consultar en el apartado *Instalación del sistema base* y *Servidores de base de datos* del *Manual de Despliegue – REF1.*
13. El acceso inicial se realizará empleando la cuenta de usuario *user* y su contraseña por defecto. **Esta contraseña se deberá modificar posteriormente, ver apartado 5.2.3 GESTIÓN DE CONTRASEÑAS**.
14. Durante el proceso de instalación, se deberá disponer de la información necesaria para configurar los siguientes parámetros:
    - Configuración de red: se modificará el fichero */etc/network/interfaces* con el direccionamiento para cada máquina (dirección IP, máscara de red, puerta de enlace y direcciones IP de los servidores DNS).
    - DNS: añadir la información DNS a */etc/resolv.conf*.
    - *Hosts*: añadir la Información de hosts a */etc/hosts*.
    - *Hostname*: añadir el nombre de la máquina a */etc/hostname*.
    - NTP: añadir la información de sincronización de hora NTP en */etc/ntp.conf.*
    - FQDN: añadir la Información de nombre y dominio al fichero en */etc/apache2/conf-available/fqdn.conf* (sólo para aquellas instalaciones donde esté instalado *apache2*).
15. Por último, se debe reiniciar el sistema para salir del *prompt* de la ISO y manejar la máquina real ya conectada a la red, mediante el comando *reboot*.
16. A partir de este punto, las máquinas serán accesibles remotamente a través de SSH.

4.6 CUENTAS POR DEFECTO

17. Las cuentas y contraseñas por defecto del producto se encuentran disponibles en el apartado *Gestión de contraseñas de las máquinas* del *Manual de Despliegue – REF1.* **Estas contraseñas se deberán emplear únicamente durante el proceso de**

despliegue del producto y se deberán modificar tan pronto como sea posible, siguiendo las indicaciones del apartado 5.2.3 GESTIÓN DE CONTRASEÑAS.

5. FASE DE CONFIGURACIÓN

5.1 AUTENTICACIÓN

18. El producto dispone de los siguientes mecanismos de autenticación para el acceso de los usuarios a la configuración:
    - Credenciales locales para el acceso con SSH, mediante usuario y contraseña. Dichas credenciales se almacenan en la base de datos propia del producto y se almacenan cifradas.
    - Servidor de autenticación externo de tipo LDAP, para el acceso al frontal web con HTTPS.
    - Credenciales locales para el acceso al frontal web con HTTPS, mediante usuario y contraseña. Dichas credenciales se almacenan en la base de datos propia del producto y se almacenan cifradas.
19. Para la autenticación de usuarios en el frontal web, se debe iniciar el módulo CAS haciendo uso del siguiente comando: *# deploy start cas.*
20. Dicho módulo hará uso por defecto de la base de datos local para la autenticación de los usuarios. En caso de emplear un servidor LDAP, se deberán seguir los pasos indicados en el apartado *Integración LDAP* del del *Manual de Despliegue – REF1*. **Se deberá evitar el uso de *simple* en el parámetro *authType***, ya que realiza el envío de contraseñas sin cifrar. Para dicho parámetro, **se recomienda el empleo de valores que hagan uso de TLS**.
21. Adicionalmente, el producto lleva a cabo la autenticación de todos sus componentes antes de comunicarse con ellos:
    - Los componentes de monitorización (agentes, colectores y *proxys*) se comunican mediante un certificado generado en cada instalación, por lo que el agente generado para monitorizar un cliente no puede ser utilizado en otro salvo que se tengan los certificados propios de cada uno de ellos. **Se recomienda modificar dichos certificados tras la instalación**, para emplear una CA de confianza de la organización, ver apartado 5.5 GESTIÓN DE CERTIFICADOS.
    - Todas las comunicaciones establecidas mediante API interna son autenticadas mediante el envío de un *TGT_Token*, generado por el sistema de autenticación de Ágata. Tanto las comunicaciones como el *token*, no son configurables.

5.2 ADMINISTRACIÓN DEL PRODUCTO

5.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

22. El producto dispone de las siguientes interfaces para la administración:
    - Administración remota de tipo CLI mediante SSHv2.

- Administración remota mediante interfaz gráfica (frontal web), haciendo uso de HTTPS con TLSv1.2. **Una vez llevadas a cabo las configuraciones iniciales, se recomienda configurar y gestionar el producto haciendo uso de esta interfaz web**.

5.2.2 CONFIGURACIÓN DE ADMINISTRADORES

23. La interfaz GUI dispone del usuario *agata* por defecto. **Este usuario se debe emplear únicamente para la configuración inicial de un usuario administrador, tras lo cual debe deshabilitarse.**
24. Para ello, ir a *Administración > Usuarios > Añadir usuario*. Crear un usuario con rol *Administrador del sistema* e introducir la contraseña deseada (ver apartado 5.2.3 GESTIÓN DE CONTRASEÑAS). Añadir el usuario a los grupos *GU-Escritorio-admin*, *GU-Escritorio-Config* y *GU-Escritorio-info* para que tenga acceso a los escritorios de configuración, administración e información.
25. Se pueden crear usuarios adicionales empleando los pasos descritos anteriormente, seleccionando el rol y escritorios deseados para limitar sus permisos.
26. Una vez configurado este usuario, desde la interfaz CLI emplear los siguientes comandos para deshabilitar el usuario *agata*:

```
# mysql -u root -p
> UPDATE `SM_Configuracion`.`USER`
SET STATE = 'DELETED'
WHERE ID_USER = 1;
```

27. El producto dispone de 4 roles predefinidos y no permite la creación de roles adicionales:
    a) Administrador de Sistema: Rol con permisos para administrar cualquier configuración y parámetro.
    b) Administrador de Empresa: Rol con permisos para administrar, a nivel empresa, todos los parámetros de configuración.
    c) Configurador: Rol con permisos, dentro de una empresa, para configurar parámetros y crear usuarios.
    d) Usuario: Rol base con privilegios para utilizar la herramienta y crear sus escritorios y páginas. No dispone de permisos para realizar la configuración o administración del producto.

5.2.3 GESTIÓN DE CONTRASEÑAS

28. Para llevar a cabo la modificación de las contraseñas de los usuarios de SSH, se deberá acceder con un usuario con permisos de administrador mediante SSH. Emplear el comando *passwd usuario*, indicando el nombre del usuario del cual se desea modificar la contraseña.

29. Para el cambio de contraseñas de usuarios del frontal web, se deberá acceder al mismo con un usuario con permisos de administrador. El cambio se realiza desde *Administración > Usuarios*.
30. Adicionalmente, **se deberá exigir la siguiente política de contraseñas de manera manual**, ya que el producto no permite su configuración:
    - Longitud mínima de 12 caracteres.
    - Incluir, al menos, una letra minúscula, una letra mayúscula, un número y un carácter especial.
    - No permitir reutilizar las últimas cinco contraseñas.
    - Tiempo de validez máximo de 60 días.
    - Obligar a cambiar la contraseña la primera vez que se acceda tras caducar esta misma.
    - No permitir un nuevo cambio de contraseña hasta pasados 10 días.

5.2.4 PARÁMETROS DE SESIÓN

31. **Se debe configurar la limitación de intentos de acceso fallidos**. Para ello, configurar el fichero *agata_zuul-des.yml*. Por defecto, está configurado para bloquear tras 3 intentos fallidos durante 2 minutos. **Se deberá modificar para aplicar un tiempo de bloqueo de 5 minutos,** modificando el parámetro *policy-list > auth > refresh-interval* a un valor de 300 segundos.
32. Una vez modificado, se deberá reiniciar el servicio empleando el siguiente comando: *# deploy restart agata-zuul.*

5.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

33. Por defecto, el producto está protegido mediante *iptables*, permitiendo únicamente el acceso a través de SSH (puerto 22) y HTTPS (puerto 443), para la interacción con los usuarios.
34. El puerto 8367 también se encuentra abierto por defecto, para las comunicaciones privadas con el proxy Ágata. **En caso de no utilizarlo, se deberá cerrar el puerto haciendo uso de los siguientes comandos**:

    iptables -D INPUT -p tcp --dport 8367 -j ACCEPT
    # dpkg-reconfigure iptables-persistent

5.3.1 CONFIGURACIÓN DEL SERVICIO *APACHE*

35. El detalle de configuración del servidor *apache* se puede consultar en el apartado *configuración frontend* del del *Manual de Despliegue – REF1.*
36. Este servicio será empleado por el producto para servir el frontal web. Por defecto emplea TLSv1.2 y redirecciona todas las peticiones HTTP (80) a HTTPS (443), por lo tanto, **no puede haber comunicaciones HTTP no cifradas**.

37. Se debe configurar un único host virtual, haciendo uso de los siguientes archivos:
    - */etc/apache2/sites-available/agata-default.conf*
    - */etc/apache2/sites-available/agata-ssl.conf*
38. Por último, se deben iniciar los siguientes microservicios y se debe iniciar el servidor:

    # deploy start agata-config

    # deploy start agata-eureka

    # deploy start agata-zuul

    # deploy start agata-ui-view

    # deploy startAll
39. Una vez iniciados, se puede acceder al frontal del producto mediante la siguiente URL: *https://<IP_FRONTAL>/agata.*

5.3.2 CONFIGURACIÓN DEL SERVICIO *POSTFIX*

40. Se emplea el servicio *Postfix* para el envío de las notificaciones sobre el estado de los servicios internos de las máquinas y las alertas que genere el producto. Actúa como intermediario SMTP entre el producto y el servidor de correo de la organización, por lo que se deberá configurar apuntando a dicho servidor.
41. El detalle de configuración del servicio *Postfix* se puede consultar en el apartado *Postfix* del *Manual de Despliegue – REF1.*
42. Se deberá llevar a cabo la configuración con autenticación mediante la configuración del fichero */etc/postfix/main.cf*. Descomentar las siguientes líneas:

    # Authentication
    smtp_sasl_auth_enable = Yes
    smtp_tls_security_level = may
    smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
    #smtp_generic_maps = hash:/etc/postfix/generic
    smtp_sasl_type = cyrus
    smtp_sasl_path = smtpd
    smtp_sasl_security_options = noanonymous
    inet_protocols = ipv4
43. Adicionalmente **se deberá añadir la siguiente línea para asegurar que se emplea siempre TLS versión 1.2 o superior**:

    smtp_tls_protocols = >= TLSv1.2

5.3.3 CONFIGURACIÓN DEL SERVICIO *MONIT*

44. *Monit* es una herramienta de *software* libre para la monitorización de procesos en sistemas Linux. El detalle de configuración del servicio *Monit* se puede consultar en el apartado *Monit* del *Manual de Despliegue – REF1.*

5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

45. Inicialmente, es necesario actualizar las claves del servidor SSH que se alojan en el directorio */etc/ssh*. Para ello se ejecutarán los siguientes comandos.

    *# rm /etc/ssh/ssh_host_ **
    # dpkg-reconfigure openssh-server
    # systemctl restart ssh
    Las claves generadas debe

46. Se debe y así viene preconfigurado:

    a) Emplear un certificado compatible con TLS 1.2 (ver apartado 5.5 GESTIÓN DE CERTIFICADOS).

    b) El uso de **protocolos de monitorización seguros**, como es el caso de SNMPv3 (ver apartado 5.8 SNMP), compatible en el producto con los estándares de seguridad necesarios en la certificación LINCE.

5.5 GESTIÓN DE CERTIFICADOS

47. El detalle de configuración de los certificados del producto se puede consultar en el apartado *Configuración frontend* del *Manual de Despliegue – REF1.*

48. En el apartado *Generación de certificados para agente, proxy y recolector* del *Manual de Despliegue – REF1* se indican los pasos para la generación de certificados propios de la instalación mediante la ejecución del script *generate_ca_and_certificate.sh*. Estos certificados serán empleados en las comunicaciones entre componentes del producto.

49. Dicho proceso genera una CA y unos certificados autofirmados. **Se recomienda emplear una CA de confianza y certificados propios**. Para ello, una vez obtenidos los tres certificados por parte de una CA de confianza, se deben almacenar estos en el servidor AGATA en */opt/agata--mdcs/etc/certs*. Dichos certificados deberán cumplir las siguientes características:

    - Tipo de clave ECDSA, con un tamaño de 256 o 384 bits.
    - Tipo de clave RSA, con una longitud de clave de 3072 bits o superior.

50. El certificado utilizado para la plataforma apache será el empleado por la interfaz GUI en las comunicaciones HTTPS para la gestión del producto. **Se deberá hacer uso de certificados propios expedidos por una CA de confianza**.

51. **Deberán seguirse los siguientes pasos generales para la configuración de los certificados para la gestión del producto**:

    - Importar el certificado de la CA que se utilizará para generar el certificado de servidor y los certificados de los agentes, *proxys* y recolectores.
    - Importar el certificado de servidor web firmado por la CA de confianza. **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.
- Tipo de clave RSA, con una longitud de clave de 3072 bits o superior.

- El CN deberá apuntar a la URL exacta que tendrá el frontal HTTPs del propio servidor: *hostname.dominio.com.*

5.6 SINCRONIZACIÓN HORARIA

52. **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*.
53. Tal como se ha visto en el apartado 4.5 INSTALACIÓN durante la instalación se incluye la información relativa al servidor NTP de la organización, de cara a sincronizar el reloj del producto.
54. **Se debe configurar la autenticación NTP**, para ello, durante el proceso de parametrización del fichero */etc/ntp.conf* debe establecerse la ubicación de las claves, mediante el uso del parámetro *keys:* del mismo.

5.7 ACTUALIZACIONES

55. Para la actualización del producto, se recibirá una notificación por parte de Ágata una vez se encuentren disponibles nuevas versiones y funcionalidades. Se pondrán a disposición los entregables correspondientes mediante repositorios seguros y se darán las instrucciones para llevar a cabo la actualización. En aquellos casos en los cuales se modifiquen parámetros de configuración y/o sea necesario llevar a cabo alguna acción, se entregará la documentación pertinente.

5.8 SNMP

56. El propio sistema de Ágata tiene la capacidad de monitorización mediante protocolo SNMP. **Se recomienda siempre que sea posible el uso de SNMPv3 con protocolos compatibles con cifrado SHA256**. No es posible forzar únicamente el empleo de SNMPv3 desde el producto, por lo que para el empleo de dicha versión deberá configurarse en los distintos componentes de la red.

5.9 ALTA DISPONIBILIDAD

57. En caso de requerir un despliegue en alta disponibilidad, deberá replicarse el servidor y llevar a cabo el balanceo de carga físico. No requiere de configuración en el producto.

5.10 AUDITORÍA

5.10.1 REGISTRO DE EVENTOS

58. Para la visualización de los eventos de seguridad, es necesario instalar una aplicación dinámica de registro. El detalle de instalación de esta se puede consultar en el apartado *Registros de auditoría* del *Manual de Despliegue – REF1.*

59. Los registros generados por el producto incluyen la fecha del evento y el usuario y acción que generan dicho registro.

5.10.2 ALMACENAMIENTO LOCAL

60. El producto almacena logs y realiza rotado de los mismos diariamente, comprimiendo los logs por tamaño (nunca superior, de forma comprimida, a 51MB) y los elimina pasados 5 días. Dado que el producto no permite el envío automático de logs a un servidor externo, **se recomienda para mayor seguridad almacenar manualmente los ficheros generados de log (ubicados en */var/log/agata_2*) en un almacenamiento externo debidamente protegido**.

5.11 COPIAS DE SEGURIDAD

61. Para llevar a cabo la configuración periódica de copias de seguridad, **se debe acceder al *cron* del sistema para descomentar la configuración de copias de seguridad semanales por defecto**:

```
# crontab –e
        #BACKUP
        @weekly /opt/agata/scripts/backup.sh 2>/dev/null
        :wq
```

62. La copia de seguridad será generada en formato *tar.gz* bajo el directorio */home/backup*. Si la copia se ha ejecutado correctamente, se generará en el mismo directorio un fichero vacío llamado *resultado_backup.txt*. En caso de producirse algún fallo en la copia de seguridad dicho fichero no será generado y Ágata generará la correspondiente alerta (siempre y cuando dicho fichero sea monitorizado).

63. Adicionalmente, **se recomienda almacenar dichas copias de seguridad en una ubicación externa**, separada del producto, para mayor seguridad. La copia de estos ficheros deberá llevarse a cabo de forma segura.

5.12 CONFIGURACIÓN DE PROXIES Y AGENTES

64. El detalle de configuración de los *proxies* y agentes se puede consultar en el apartado *Despliegue y configuración de proxies y agentes* del del *Manual de Despliegue – REF1.*

65. Se emplean dichos *proxies* para subir los datos que se monitorizan de los distintos activos de la plataforma al *Core*. Los datos son proporcionados al proxy Maestro a

través de los recolectores, que son los que levantan los *plugins* necesarios en los servidores que tengan el Agente instalado.

66. Para el correcto funcionamiento, se deben configurar los certificados del agente, el proxy y el colector, tal como se indica en el apartado 5.5 GESTIÓN DE CERTIFICADOS.

6. FASE DE OPERACIÓN

68. En la fase de operación se deben realizar las siguientes actividades:

- Almacenamiento: si bien Ágata puede auto monitorizarse, es responsabilidad del Administrador de Sistemas que haya espacio suficiente en disco para que se pueda operar con normalidad. Para ello, se deben **almacenar las copias de seguridad periódicas en ubicaciones externas y revisar que haya suficiente espacio disponible en el producto.**
- Housekeeping: se debe mantener el volumen de datos adecuado, y para ello se deberá realizar un borrado o extracción de datos de las colecciones de Mongo de persistencia de valores de propiedades, fijando una **política de prevalencia**, para mantener la aplicación con una cantidad de datos constante y no incurrir en errores de desbordamientos de memoria.
- Sistema Operativo y actualizaciones: el Administrador de Sistema debe mantener al día con las **últimas versiones de Sistema Operativo Debian** para garantizar los servicios de actualización y recibir y a**plicar los parches de seguridad** pertinentes del producto.
- Registros de Auditoría: estos registros, al igual que los de las propiedades, deben **mantenerse de una manera periódica** y delimitar muy bien los accesos al mismo. Se **realizará una revisión** periódica al menos de los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

7. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la integridad del paquete	☐	☐	
CONFIGURACIÓN			
Configuración de usuarios	☐	☐	
Actualización de contraseñas de usuarios	☐	☐	
Borrado usuario *agata*	☐	☐	
Configuración de la política de contraseñas	☐	☐	
Configuración de los parámetros de sesión	☐	☐	
Importar CA, crear e importar certificados	☐	☐	
Sincronización de la hora de los sistemas	☐	☐	
No utilizar versiones inferiores a SNMPv3	☐	☐	
Almacenamiento externo de logs	☐	☐	
Configuración de las copias de seguridad periódicas	☐	☐	
CONFIGURACIÓN			
Vigilancia del espacio disponible en disco	☐	☐	
Creación de política de prevalencia de datos	☐	☐	
Actualización del Sistema Operativo	☐	☐	
Mantenimiento y revisión de logs	☐	☐	

8. REFERENCIAS

69. Los manuales del producto son privados y, por lo tanto, facilitados a la organización tras la adquisición del producto.

REF1 *Instrucciones de Despliegue Agata Standalone V7.11.pdf*

9. ABREVIATURAS

API	*Application Programming Interface*
CA	*Certificate Authority*
CLI	*Command-Line Interface*
CPD	Centro de Procesamiento de Datos
ENS	Esquema Nacional de Seguridad.
GUI	*Graphical User Interface*
HTTPS	*HyperText Transfer Protocol Secure*
LDAP	*Light Directory Access Protocol*
NTP	*Network Time Protocol*
SNMP	*Simple Network Monitoring Protocol*
SSH	*Secure SHell*
TIC	Tecnologías de la Información y la Comunicación
TLS	*Transport Layer Security*

PUBLICACIONES DE DEFENSA

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