centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 1444

## Procedimiento de Empleo Seguro
## FortiAnalyzer


Julio 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


NIPO: 083-23-282-9.
Fecha de Edición: julio 2023.

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
2024.01.15 12:08:10 +01'00'

**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**
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

# ÍNDICE

# 1. INTRODUCCIÓN

1. Este documento tiene como objetivo mostrar l**as funcionalidades de seguridad de FortiAnalyzer, la solución para centralización de logs, análisis e informes de Fortinet.**
2. La familia de productos FortiAnalyzer extiende las capacidades de visibilidad, gestión de alarmas y eventos de las plataformas FortiGate, FortiCarrier, FortiAP, FortiWeb, FortiMail, FortiCache, FortiSandbox, FortiManager, FortiDDOS y FortiClient, así como de otros dispositivos de terceros compatibles con Syslog.
3. Un conjunto de informes fácilmente configurables permite analizar, reportar y almacenar eventos de seguridad, tráfico de red, contenido web y mensajes para medir el cumplimiento de políticas de una organización.
4. A continuación, se indican algunas de las funcionalidades de FortiAnalyzer:
    - Más de 550 informes en distintos idiomas y gráficos configurables ayudan a monitorizar y mantener identificados patrones de ataques, políticas de uso aceptable y a demostrar el cumplimiento de políticas.
    - Informes de capacidad y utilización de la red, que permiten gestionar las redes de forma planificada y eficiente.
    - Funcionalidades avanzadas, tales como la correlación de eventos, análisis forense y vulnerabilidades de los activos, proporcionan herramientas esenciales para una defensa en profundidad en redes complejas.
    - Segmentación de la información generada por los dispositivos en dominios administrativos permitiendo modelos de delegación basados en roles o tipo MSSP.
    - Ciclo completo de gestión de la información que abarca los procesos de recolección, normalización, clasificación, correlación y explotación en modo de alertas e informes.
    - Hasta 24 TB de capacidad para almacenar logs, así como elegir entre diferentes niveles de RAID (0, 1, 5, 6, 10, 50 y 60), discos en *spare*, e intercambio de discos en caliente, permiten asegurar los datos para cumplir con las necesidades de la organización.
    - Soporte IPv6, tanto para la recepción de logs como para el acceso de administración a la plataforma.
    - Ejecución de diferentes utilidades de diagnóstico, tales como: *ping*, *traceroute* y visor de logs.
    - Posibilidad de despliegue de la plataforma en entornos virtuales.
    - Servicios de integración web desde terceras aplicaciones con *Web Services*.
    - Múltiples usuarios de administración con diferentes perfiles de gestión administrativa basada en roles.

## 2. OBJETO Y ALCANCE

5. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución **FortiAnalyzer en su versión 6.2** (v6.2.8-build9589 o superior).
6. El presente documento aplica la versión FAZ-VM y a los modelos Hardware:
   - FAZ-800F
   - FAZ-1000F
   - FAZ-2000E
   - FAZ-3000F
   - FAZ-3500G
   - FAZ-3700F
7. **Este producto cualificado e incluido dentro de la Familia de Sistemas de Gestión de Eventos de Seguridad del Catálogo de Productos y Servicios de Seguridad STIC del CCN (CPSTIC).**

## 3. ORGANIZACIÓN DEL DOCUMENTO

8. Este documento se compone de los siguientes apartados:

   a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, durante la 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 PREVIA A LA INSTALACIÓN

## 4.1 ENTREGA SEGURA DEL PRODUCTO

9. El dispositivo se entrega en formato *appliance*. Tras la entrega del dispositivo, es necesario verificar que no ha sido manipulado. Para asegurarse de la autenticidad e integridad del producto se deben seguir los siguientes pasos:
    - Verificar que el embalaje contiene los cierres originales del fabricante.
    - Verificar que el embalaje se encuentra en condiciones óptimas, sin golpes ni signos de humedad o deterioro. El embalaje interno deberá ser una bolsa de plástico transparente sellada.
    - Verificar con la información comercial (documento *pdf* del pedido) que el Número de Serie del equipo corresponde con el recibido.
    - Verificar que el sello de garantía está intacto.

## 4.2 ENTORNO DE INSTALACIÓN SEGURO

10. Se recomienda llevar a cabo la instalación de FortiAnalyzer en el CPD de la organización con el fin de limitar el acceso físico al equipo. El acceso físico al producto deberá realizarse únicamente por administradores previamente autorizados.

## 4.3 REGISTRO Y LICENCIAS

11. Para acceder al firmware y el soporte de usuario, se debe registrar el producto en la página de Soporte de Fortinet. En el siguiente enlace se pueden consultar los pasos concretos necesarios para llevar a cabo dicho registro.

## 4.4 CONSIDERACIONES PREVIAS

12. Se recomienda la ejecución de las *Best Practices* proporcionadas por Fortinet en la implementación del sistema FortiAnalyzer, las cuales se pueden consultar en el siguiente enlace. Adicionalmente, se recomienda situar el dispositivo detrás de un cortafuegos, para limitar los intentos de acceso no autorizados al mismo.
13. Durante el acceso inicial al dispositivo, se solicitará configurar la contraseña del usuario *admin*. Se deberán seguir las recomendaciones indicadas en el apartado **5.4.3 PARÁMETROS DE SEGURIDAD**, relativas a la política de contraseñas.
14. **Se deberá desactivar el usuario por defecto administrador de API**. Para ello, mediante consola, ejecutar los siguientes comandos:

```
config system admin user
   edit admin
   set rpc-permit none
end
```

## 4.5 INSTALACIÓN

15. El producto debe emplear la versión **FortiAnalyzer v6.2.8 o superior**, por lo que será necesario descargar e instalar esta mediante los siguientes pasos:
    - Ir al enlace https://support.fortinet.com/ y acceder con la cuenta de la organización, recibida el registrar el equipo en la página de soporte del producto.
    - Navegar hasta la página de descarga de *FortiAnalyzer 6.2 FIPS-CC Certified*.
    - Descargar el fichero *firmware* correspondiente al hardware adquirido.
    - Para verificar la integridad del *software* descargado, **realizar el hash SHA-512 del fichero y verificar que corresponde con el indicado en la página de descarga**, bajo *Get Checksum Code*.
    - Por último, seguir los pasos indicados en el apartado *Upgrading FortiAnalyzer* de la guía *Upgrade Guide – REF2.*
16. Durante el arranque inicial del producto, se recomienda llevar a cabo las instrucciones contenidas en el apartado *Setting up FortiAnalyzer* de la guía *Administration Guide – REF1*.

# 5. FASE DE CONFIGURACIÓN

## 5.1 MODO DE OPERACIÓN SEGURO

17. El producto requiere de la configuración del token de entropía *Araneus Alea II*. Este se emplea para la generación segura de claves, así como fuente confiable de valores aleatorios. Adicionalmente, se debe activar el modo de operación seguro.

18. Para llevar a cabo la instalación del token, este se debe conectar a un puerto USB disponible del producto. Una vez conectado, **se deben introducir los siguientes comandos mediante consola, que servirán para configurar el token y activar el modo seguro simultáneamente**:

```
config system fips
   set status enable
   set entropy-token enable
end
```

19. Una vez introducidos los comandos, el dispositivo solicitará la contraseña de administrador. Aceptar los cambios e introducir el comando *get system status* para verificar que el modo seguro ha sido activado. Para ello se deberá observar la siguiente línea: *FIPS mode: enabled*.

20. En modo seguro, el producto deshabilita el empleo de HTTP y Telnet como métodos de acceso remotos, permitiendo únicamente el uso de protocolos seguros.

21. Se recomienda configurar el periodo de *re-seed* en 60 minutos, ya que por defecto es cada 24 horas. Para ello:

```
config system fips
   set re-seed-interval 60
end
```

### 5.1.1 CIFRADO DE DATOS

22. **Se deberá habilitar el cifrado de datos y cargar una clave para llevarlo a cabo**. Este cifrado afectará a los Parámetros de Seguridad Críticos. Para ello, emplear los siguientes comandos mediante la consola:

```
configure system global
   set private-data-encryption enable
end
```

23. Una vez habilitado el cifrado de datos, el producto solicitará al administrador una clave AES de 128 bits, la cual será empleada para llevar a cabo el cifrado.

## 5.2 AUTENTICACIÓN

24. Desde la consola web de administración es posible monitorizar los diferentes usuarios de administración que se encuentren conectados en cada momento a FortiAnalyzer, siendo posible desconectar a dichos usuarios en caso necesario. Se

muestra tanto la dirección IP del usuario de administración y el tipo de acceso (GUI, CLI), como la fecha y hora de la conexión.

25. Dicha monitorización se realiza desde *Systems Settigs > Dashboard*, dentro del **widget** de *System information*, hacer clic en el icono de lista junto a *Current Administrators*.
26. El producto requiere la autenticación de usuarios para la gestión. Los mecanismos de autenticación empleados por el producto son los siguientes:
    - Credenciales locales, mediante usuario y contraseña. Dichas credenciales se almacenan en el producto. Para la creación y gestión de usuarios locales, ver el apartado **5.4.2 CONFIGURACIÓN DE ADMINISTRADORES**.
    - Servidor de autenticación externo. Mediante la integración con distintos servidores de autenticación. Para la configuración de dichos servidores, ver apartado **5.3 SERVIDORES DE AUTENTICACIÓN**.
27. Se recomienda **emplear únicamente la autenticación local** como método de autenticación de usuarios.

## 5.3 SERVIDORES DE AUTENTICACIÓN

28. En caso de requerir la configuración de un servidor externo de autenticación, consultar el apartado *Authentication* de la guía *Administration Guide – REF1*.
29. Para servidores LDAP, se deberá habilitar *secure connection* y seleccionar el protocolo LDAPS o STARTTLS.

## 5.4 ADMINISTRACIÓN DEL PRODUCTO

### 5.4.1 ADMINISTRACIÓN LOCAL Y REMOTA

30. El producto dispone de las siguientes interfaces para la administración:
    - Administración local por consola.
    - Administración remota de tipo CLI mediante SSH o Telnet. **Para este tipo de administración, se deberá emplear únicamente SSH**.
    - Administración remota de tipo GUI mediante HTTPS. Este tipo de administración se encuentra deshabilitada por defecto, por lo que deberá habilitarse durante la configuración del producto, consultar apartado **5.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS**. **Se deberá configurar también el producto para forzar el empleo de TLS versión 1.2 o superiores**, para ello consultar el apartado **5.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS**.
31. Tal como se ha visto en el apartado **5.1 MODO DE OPERACIÓN SEGURO**, el producto deshabilita Telnet y HTTP como métodos de administración remota al activar el modo de empleo seguro.

### 5.4.2 CONFIGURACIÓN DE ADMINISTRADORES

32. El detalle de configuración de administradores se puede consultar en el apartado *Administrators* de la guía *Administration Guide – REF1.*

33. Para crear un nuevo usuario, ir a *System Settings > Admin > Administrators* y seleccionar *Create New*. El parámetro *Admin Type* se deberá configurar con el valor *Local*. Seleccionar la casilla *Force this administrator to change password upon next logon*, de tal forma que deba modificar su contraseña en el primer acceso.

34. Los privilegios de acceso de los administradores se definen a través de un perfil de administración. Por defecto el sistema proporciona tres (3) perfiles de acceso con diferentes niveles de acceso:

    - ***Restricted_user***: No dispone de privilegios de acceso al sistema y solo puede ver todos los dispositivos asociados.
    - ***Standard_user***: No dispone de privilegios de acceso al sistema y puede ver y modificar sobre todos los dispositivos asociados.
    - ***Super_user***: Dispone de privilegios completos al sistema y a los dispositivos.

35. Adicionalmente se pueden crear perfiles de administración nuevos, en los que se pueden determinar los permisos específicos. Para ello ir a *System settings > Admin > Profile* y seleccionar *Create new*.

### 5.4.3 PARÁMETROS DE SEGURIDAD

36. Se deberá establecer un tiempo de inactividad, después del cual se desconecte a los usuarios. Para ello, desde *Admin > Admin Settings,* configurar los distintos parámetros *Idle Timeout* en un valor de cinco minutos (300 segundos).

37. El producto permite limitar el acceso de los usuarios administradores desde uno o varios dispositivos únicamente. Para ello ir a *Admin > Administratior > (usuario)*:

38. Se debe configurar una política de contraseñas segura. Para ello ir a *Admin > Admin Settings > Password Policy* y configurar los siguientes parámetros:

    - Activar la casilla *Password Policy*.
    - *Minimum Lenght*: establecer un valor de 12 caracteres de longitud mínimo.
    - *Must Contain*: activar todas las casillas para forzar el empleo de, al menos, una letra mayúscula, una minúscula, un número y un carácter especial.
    - *Admin Password Expires after*: establecer un valor de 60 días, tras el cual se deberá modificar la contraseña de usuario.

39. Adicionalmente el administrador del sistema **deberá exigir a los usuarios la siguiente política de contraseñas de manera procedural**:

    - No reutilizar las últimas 5 contraseñas.
    - No permitir un nuevo cambio de contraseñas antes de pasados 10 días.

40. Se debe configurar el bloqueo de cuentas de usuarios tras tres intentos fallidos de acceso, durante cinco minutos. Para ello, emplear los siguientes comandos:

```
config system global
set admin-lockout-threshold 3
set admin-lockout-duration 300
end
```

### 5.4.4 CONFIGURACIÓN DEL BANNER DE ACCESO

41. Se debe configurar el mensaje de aviso antes de la autenticación en el producto. Para ello, se deben emplear los siguientes comandos para habilitar el mensaje y configurar su contenido:

```
config system global
   set pre-login-banner enable
   set pre-login-banner-message <texto>
end
```

## 5.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

42. Por defecto, el acceso remoto a la plataforma se encuentra desactivado. Por ello, se deberá habilitar el acceso remoto mediante HTTPS. Para ello, se puede configurar la interfaz port1 para permitir el acceso mediante HTTPS y SSH, por ejemplo:

```
config system interface
   edit port1
   set allowaccess https ssh
end
```

43. Posteriormente, desde la interfaz GUI, es posible configurar todas las interfaces (*System Settings > Network*). **Se recomienda deshabilitar todas aquellas que no vayan a emplearse**. Para aquellas en uso, se deberá limitar los protocolos a *HTTPS, SSH* y *Web Service*.

## 5.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

44. SSHv1 se encuentra deshabilitado por defecto usándose únicamente SSHv2.

45. Se deberá configurar el grupo *Diffie-Hellman* empleado por el producto empleando los siguientes comandos. El producto dispone de distintas opciones, **se recomienda emplear 3072 bits.**

```
config sytem global
   set dh-params 3072
end
```

46. Se deberá configurar el producto para emplear únicamente algoritmos y versiones de TLS seguras. Para ello emplear los siguientes comandos:

```
config system global
set fgfm-ssl-protocol [tlsv1.2 or tlsv1.3]
set oftp-ssl-protocol [tlsv1.2 or tlsv1.3]
```

```
set ssl-protocol [tlsv1.2 or tlsv1.3]
set webservice-proto [tlsv1.2 or tlsv1.3]
set ssl-low-encryption disable
end

config fmupdate fds-setting
set fds-ssl-protocol [tlsv1.2 or tlsv1.3]
end
```

## 5.7 GESTIÓN DE CERTIFICADOS

47. El detalle de configuración de los certificados se puede consultar en el apartado *Certificates* de la guía *Administration Guide – REF1*. El producto emplea un único certificado de servidor para las comunicaciones de la interfaz GUI a través de HTTPS y con el servidor externo de auditoría a través de TLS.

48. **Deberán seguirse los siguientes pasos generales**:

    - Importar el certificado de la CA que se utilizará para generar el certificado de servidor. Deberá incluir las extensiones *Basic Constraint X509* y *CRLSign* con valor *True*.
    - 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 bits o superior.
    - Importar el certificado de servidor una vez recibido.
    - Se recomienda configurar la lista de revocación de certificados (CRL) correspondiente, para permitir al producto verificar el estado de los certificados.

## 5.8 SINCRONIZACIÓN HORARIA

49. **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*.

50. Se deberá deshabilitar el protocolo NTP de sincronización horaria debido a que no permite el uso de claves de autenticación. Para ello, emplear los siguientes comandos:

```
config system ntp
   set status disable
end
```

51. Por lo tanto, se recomienda emplear la hora local del dispositivo. Para ello, ir a *System Settings > Dashboard* y pulsar sobre el icono de *System Information* y después sobre el botón de editar al lado de *System time*. Finalmente configurar los valores de *Time Zone* y *Set Time*.

## 5.9 ACTUALIZACIONES

52. El producto permite la actualización manual del *Firmware* desde un fichero descargado en el dispositivo del administrador o directamente desde el servicio de conexión segura *FortiGuard* de Fortinet. El detalle sobre el proceso de actualización se puede consultar en la guía *Upgrade Guide – REF2*.

53. Una vez descargado el paquete de *firmware,* **se debe verificar la integridad del paquete de firmware descargado mediante su hash SHA-512**. Este debe coincidir con el mostrado en la página de descarga.

## 5.10 AUTO-CHEQUEOS

54. El producto dispone de una serie de pruebas, durante el arranque o bajo ciertas condiciones, que verifican el correcto funcionamiento de los algoritmos criptográficos y la integridad del firmware.

55. Adicionalmente, un usuario administrador puede ejecutar dichos test manualmente en cualquier momento. Para ejecutar todas las pruebas, emplear el comando *execute fips kat all*. En caso de desear ejecutar solo una prueba específica, *execute fips kat <test_name>*.

56. En caso de fallar alguno de los chequeos de algoritmos criptográficos, el dispositivo procederá a apagarse, impidiendo así su uso. En caso de entrar en modo de *error*, el producto entrará en un modo seguro que no permitirá el paso de datos.

## 5.11 ALTA DISPONIBILIDAD

57. El producto permite configurar un clúster de alta disponibilidad (HA) que proporcionará las siguientes características:

    - Redundancia en tiempo real en caso de que falle una unidad principal de FortiAnalyzer. Si falla la unidad principal, se selecciona otra unidad del clúster como unidad principal.
    - Sincroniza los registros y datos de forma segura entre múltiples unidades FortiAnalyzer y sincroniza los siguientes módulos de configuración:
        - Incidentes y Eventos.
        - Informes.
        - Configuración del Sistema basada en la siguiente tabla:
    - Alivia la carga en la unidad principal mediante el uso de unidades de respaldo para procesos como la ejecución de informes.

58. Un clúster de FortiAnalyzer HA puede tener un máximo de cuatro unidades: **una unidad principal con hasta tres unidades de respaldo**. Todas las unidades del clúster deben ser de la misma serie de FortiAnalyzer. Todas las unidades son visibles en la red.

59. Todas las unidades deben funcionar en el mismo modo de funcionamiento: Analizador o Colector.

60. Debido a limitaciones técnicas, la implementación actual de FortiAnalyzer HA no es compatible con algunas infraestructuras de nube pública, como Microsoft Azure, Google Cloud Platform o AWS. FortiAnalyzer HA solo funciona en configuraciones donde se permite VRRP.

61. El detalle de configuración de Alta disponibilidad de FortiAnalyzer se puede consultar en el apartado *High Availability* de la guía *Administration Guide – REF1.*

## 5.12 AUDITORÍA

### 5.12.1 REGISTRO DE EVENTOS

62. El producto genera registros de auditoría para las distintas acciones realizadas por los usuarios. Estos están almacenados en la memoria o en el disco duro interno y se pueden consultar desde *System Settings > Event Log*.

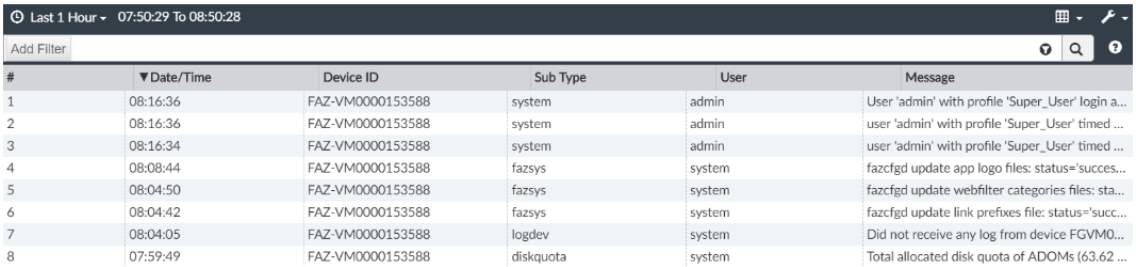


**Ilustración 1. Eventos de auditoría**

63. Desde *System Settings > Advanced > File Management*, se pueden configurar los periodos de retención de los registros de auditoría.

64. El detalle de configuración de los registros de auditoría se puede consultar en el apartado *Event Log* de la guía *Administration Guide – REF1*.

65. El producto permite el envío de los registros de auditoría a un servidor externo mediante Syslog. Sin embargo, dicho envío se realiza en claro por lo que, **en caso de emplearse, deberá situarse el servidor al que se envíen los registros en la misma red local que el producto**.

66. Para configurar el envío de registros a un servidor de auditoría externo, ir a *System Settings > Advanced > Syslog Server* e introducir los datos del servidor al que se desea realizar el envío de registros. Por último, se deberán emplear los siguientes comandos para habilitar el envío de registros a dicho servidor:

```
config system locallog syslogd setting
set severity information
set status enable
set syslog-name <syslog server name>
end
```

67. El producto permite también la exportación de logs de forma manual, a través de SFTP. Para ello se debe ejecutar el siguiente comando mediante consola:

```
execute backup logs <device name(s)> sftp <ip> <username> <passwd>
<directory> [vdlist]
```

68. Es posible programar el envío a una hora concreta cada día o en el momento de la rotación del fichero de logs. Esto se debe realizar desde *System Settings > Advanced > Device Log Setting*, **se deberá emplear SFTP**.

## 5.13 COPIAS DE SEGURIDAD

69. **Se recomienda realizar copias de seguridad periódicas de la configuración del producto** para, en caso de ser necesario, poder recuperar el estado de la máquina. Para ello es posible crear copias de seguridad locales. Será recomendable llevar copias de seguridad a cabo tras un cambio de configuración relevante.

70. Dichas copias pueden llevarse a cabo manualmente o con una periodicidad programada. Para hacer una copia de seguridad de la configuración de FortiAnalyzer, ir a *System Settings > System Information (widget) > Backup*. Activar la casilla *Encryption* para almacenar las copias cifradas e introducir la contraseña deseada.

71. En caso de necesitar restaurar el sistema a partir de una copia de seguridad, ir a *System Settings > Dashboard > System Information (widget)*. Pulsar sobre el botón de restauración, próximo a *System Configuration* y seleccionar el archivo de copia de seguridad que se desea restaurar.

## 5.14 FUNCIONES DE SEGURIDAD

### 5.14.1 MODOS DE OPERACIÓN

72. El producto se puede configurar en tres (3) modos diferentes de operación:

- **Analizador**: El modo por defecto con alta disponibilidad configurada, que soporta todas las funcionalidades de FortiAnalyzer. Este modo combina los distintos logs recibidos de uno o más colectores.
- **Standalone**: El modo por defecto sin alta disponibilidad configurada, en el que el dispositivo realiza las funciones de analizador y/o recolector.
- **Colector**: El modo utilizado para almacenar y reenviar logs a otro dispositivo FortiAnalyzer en modo Analizador. En lugar de escribir los logs en su base de datos, el colector puede retener los logs en su formato original (binario) para su envío. En este modo, la función de informes y otras utilidades están deshabilitadas.

73. El modo Colector se usa para incrementar las prestaciones de FortiAnalyzer en grandes entornos. El Colector proporciona un buffer para el analizador, ya que le descarga la tarea de recepción de logs. Debido a que la tarea de recolección de logs de los dispositivos conectados es llevada a cabo por el colector, los ratios y velocidad de recepción de logs por segundo son superiores.

74. El detalle de configuración de estos modos se puede consultar en el apartado *Collectors and Analyzers* de la guía *Administration Guide – REF1.*

75. En el siguiente gráfico, se muestra el flujo de trabajo de FortiAnalyzer para el almacenamiento de logs, análisis y creación de informes:

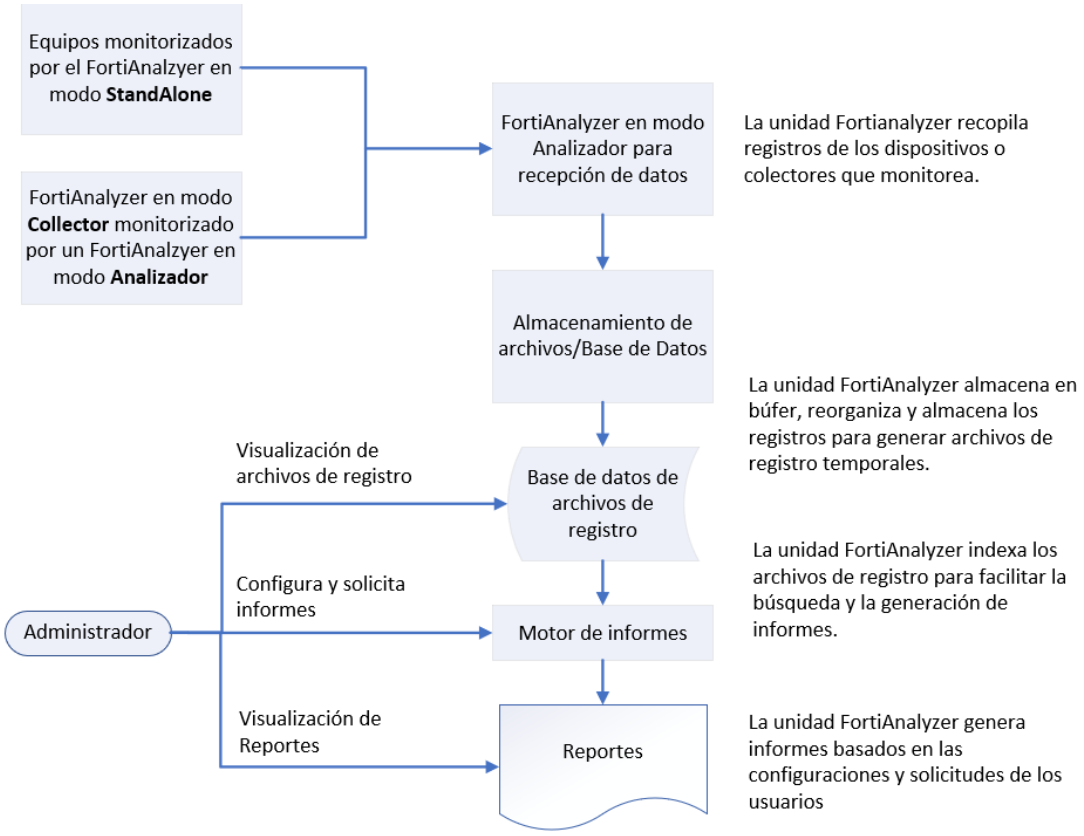


**Ilustración 2. Flujo de trabajo.**

76. Los registros y archivos se almacenan en los discos de FortiAnalyzer. Los registros también se almacenan temporalmente en la base de datos SQL.

77. FortiAnalyzer almacena los logs e informes en formato SQL. Los logs se insertan en la base de datos SQL local para la posterior generación de informes.

78. Es posible configurar una política de datos y la configuración de utilización del disco para los dispositivos:

- Política de Datos: empleada para controlar cuánto tiempo mantener los registros indexados y comprimidos. Cuando los ADOM están habilitados, puede especificarse configuraciones para cada ADOM y las configuraciones se aplican a todos los dispositivos en ese ADOM. Cuando los ADOM están deshabilitados, la configuración se aplica a todos los dispositivos administrados.
- Configuración de Utilización de Disco: En FortiAnalyzer, el sistema reserva del 5% al 20% del espacio en disco para el uso del sistema y el desbordamiento inesperado de la cuota. El 80% al 95% restante del espacio en disco está disponible para la asignación a dispositivos.

79. La configuración de las políticas de datos y el uso de disco se puede consultar en el apartado *Log Storage* de la guía *Administration Guide – REF1*.

80. El producto posee la capacidad de realizar el envío de los registros recolectados a otro sistema de Syslog externo, pudiendo filtrar mediante reglas de *Forwarding* qué eventos y de que dispositivos son enviados y garantizando la conexión mediante el uso de certificados Local o Peer.

81. Para llevar a cabo la configuración del Servidor Externo Syslog, ir a *System Settings > Advanced > Syslog Server*.

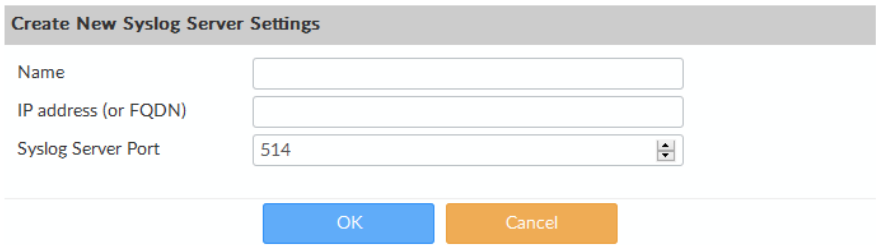


**Ilustración 3. Configuración del reenvío de eventos.**

82. Para configurar las reglas de *Log Forwarding*, ir a *System Settings > Log Forwarding*.

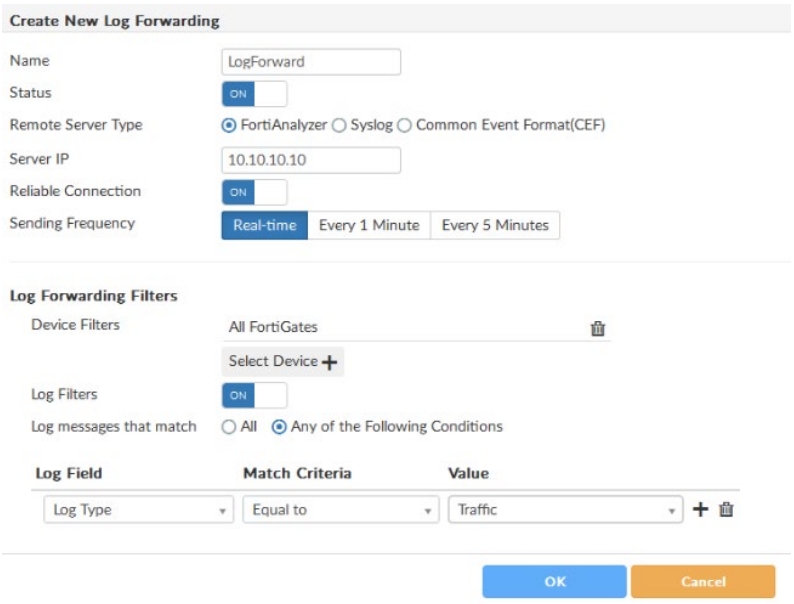


**Ilustración 4. Configuración de Log Forwarding.**

### 5.14.2 DOMINIOS ADMINISTRATIVOS

83. El producto permite la creación de dominios administrativos (ADOMs), empleados para agrupar los productos gestionados y permitir una gestión más simple y centralizada, pudiendo modificar todos los dispositivos de un dominio simultáneamente.

84. El detalle de configuración de los dominios se puede consultar en el apartado *Administrative domains* de la guía *Administrative Guide – REF1*.

### 5.14.3 GENERACIÓN DE EVENTOS

85. El producto permite generar, monitorizar y gestionar alertas y eventos a partir de los registros recolectados.
86. Para poder generar eventos, se deben configurar los controladores de eventos. Estos controladores serán los encargados de generar y alertar de los eventos en base a los registros recolectados.
87. El detalle de configuración de los eventos se puede consultar en el apartado *Incident and Event Management* de la guía *Administration Guide – REF1.*

## 6. FASE DE OPERACIÓN

88. Durante la fase de operación del producto, el administrador debe llevar a cabo las siguientes tareas de mantenimiento:

- Verificar regularmente la existencia de nuevo *firmware* para mantenerlo actualizado.
- En caso de conexión de múltiples administradores de forma simultánea verificar identidad de dichos administradores:

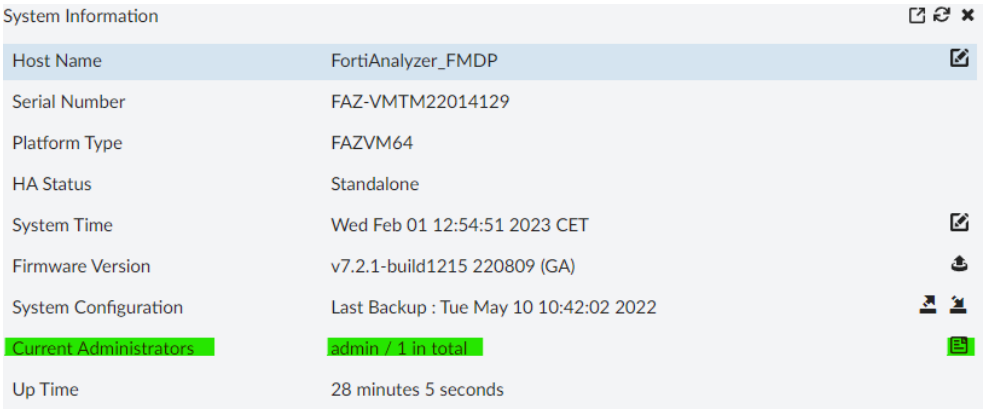


**Ilustración 5. Verificación conexión de administradores.**

- Verificar regularmente que no se excede la cantidad de logs/día adquirido en la licencia.
- Comprobaciones periódicas del *hardware* y *software* para asegurar que no se ha introducido hardware o software no autorizado.
- Mantenimiento de los registros de auditoría.

## 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 | ☐ | ☐ | |
| Configuración del cifrado de disco | ☐ | ☐ | |
| **ADMINISTRACIÓN DEL PRODUCTO** | | | |
| Configuración de roles y usuarios | ☐ | ☐ | |
| Configuración de la política de contraseñas | ☐ | ☐ | |
| Configuración de los parámetros de sesión | ☐ | ☐ | |
| **CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS** | | | |
| Deshabilitar las interfaces y servicios no empleados | ☐ | ☐ | |
| **CONFIGURACIÓN DE PROTOCOLOS SEGUROS** | | | |
| Configuración de TLSv1.2 | ☐ | ☐ | |
| Configuración de SSHv2 | ☐ | ☐ | |
| **GESTIÓN DE CERTIFICADOS** | | | |
| Importar CA, crear CSR e importar el certificado de servidor | ☐ | ☐ | |
| **COPIAS DE SEGURIDAD** | | | |
| Creación de los *backups* | ☐ | ☐ | |
| **AUDITORÍA** | | | |
| Configuración del envío de los logs a un servidor *Syslog* | ☐ | ☐ | |

## 8. REFERENCIAS

89. El enlace principal de guías del producto contiene acceso a toda la documentación: https://docs.fortinet.com/product/fortianalyzer/6.2

REF1 Administration Guide

https://docs.fortinet.com/document/fortianalyzer/6.2.8/administration-guide/366418/setting-up-fortianalyzer

REF2 Upgrade Guide

https://docs.fortinet.com/document/fortianalyzer/6.2.8/upgrade-guide/427568/introduction

## 9. ABREVIATURAS

| | |
|---|---|
| **ADOM** | *Administrative Domain (Dominios Administrativos)* |
| **API** | *Application Programming Interface* |
| **CCN** | Centro Criptológico Nacional |
| **CLI** | *Command Line Interface* |
| **CPD** | Centro de Proceso de Datos |
| **CPSTIC** | Catálogo de Productos y Servicios TIC |
| **CRL** | *Certificate Revocation List* |
| **ENS** | Esquema Nacional de Seguridad. |
| **FMG** | *FortiManager* |
| **GUI** | *Graphical User Interface* |
| **HA** | *High Availability* |
| **HTTPS** | *Hypertext Transfer Protocol Secure* |
| **NTP** | *Network Time Protocol* |
| **SMTP** | *Simple Mail Transfer Protocol* |
| **SSH** | *Secure Shell* |
| **TLS** | *Transport Layer Security* |
| **URL** | *Uniform Resource Locator* |
| **VM** | *Virtual Machine* |
| **VPN** | *Virtual Private Network* |

PUBLICACIONES DE DEFENSA

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