centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1213

Procedimiento de Empleo Seguro
WatchGuard Advanced EPDR



Noviembre 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

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.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 3
2 OBJETO Y ALCANCE 4
3 ORGANIZACIÓN DEL DOCUMENTO 5
4 FASE PREVIA A LA INSTALACIÓN 6
4.1 ENTREGA SEGURA DEL PRODUCTO 6
4.2 ENTORNO DE INSTALACIÓN SEGURO 6
4.3 REGISTRO Y LICENCIAS 6
4.4 CONSIDERACIONES PREVIAS 7
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 7
5 FASE DE INSTALACIÓN 9
6 FASE DE CONFIGURACIÓN 10
6.1 MODO DE OPERACIÓN SEGURO 10
6.2 AUTENTICACIÓN 11
6.2.1 AUTENTICACIÓN BÁSICA 11
6.2.2 AUTENTICACIÓN DE DOS FACTORES 11
6.3 ADMINISTRACIÓN DEL PRODUCTO 12
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 12
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 12
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 12
6.5 GESTIÓN DE CERTIFICADOS 13
6.6 SERVIDORES DE AUTENTICACIÓN 13
6.7 SINCRONIZACIÓN 13
6.8 ACTUALIZACIONES 13
6.9 AUTO-CHEQUEOS 13
6.10 ALTA DISPONIBILIDAD 14
6.11 AUDITORÍA 14
6.11.1 REGISTRO DE EVENTOS 14
6.11.2 ALMACENAMIENTO LOCAL 14
6.11.3 ALMACENAMIENTO REMOTO 14
6.12 BACKUP 15
7 REFERENCIAS 16
8 ABREVIATURAS 17

ILUSTRACIONES

Ilustración 1 Estructura de WatchGuard Advanced EPDR 4
Ilustración 2 Entorno operacional de WatchGuard Advanced EPDR 8

1 INTRODUCCIÓN

WatchGuard Advanced EPDR es una solución en nube alojada en la infraestructura de WatchGuard que permite proteger activos de IT. Lleva a cabo funciones como proteger los puntos finales de las amenazas y reducir la superficie de ataque. Previene, detecta y responde al malware conocido y desconocido, así como a los ataques sin archivos y sin malware (ataques sin el uso de un archivo).

Está formado por los siguientes componentes:

a) **WatchGuard Cloud Console:** Es la plataforma global donde los productos de WatchGuard son gestionados, incluyendo la presente solución. Esta plataforma proporciona identificación y autenticación a los usuarios autorizados, así como la gestión de sus roles. Se subdivide en los siguientes elementos:

   i. **WatchGuard Endpoint:** Representa la colección de componentes en nube que se encargan de la gestión de los WatchGuard Agents instalados en los dispositivos finales, previniendo, detectando y respondiendo ante amenazas. Estos componentes son: *WebAPI, Command Hub, Endpoint API, Knowledge Delivery, File Upload* y *Storage*.

   ii. **Admin Web Interface**: Representa la interfaz web a la que acceden los usuarios autorizados para gestionar los WatchGuard Agents en los dispositivos finales de la infraestructura del cliente. Esta interfaz web interactúa con la WebAPI para la comunicación con el resto de los componentes de Watchguard mencionados anteriormente.

b) **WatchGuard Agent**: Este agente se instala en los dispositivos finales y detecta amenazas en ellos, actuando como un antivirus. Está compuesto por dos componentes:

   i. **WatchGuard Windows Agent:** Este componente proporciona funcionalidades de gestión incluyendo despliegue y configuración de agentes, sincronización con componentes de WatchGuard Endpoint e informe de estado.

   ii. **WatchGuard Windows Protection:** Este componente implementa funcionalidades de monitorización, detección y respuesta y se comunica con los componentes de WatchGuard Endpoint para la carga de archivos y recuperación de firmas.

En la siguiente figura se muestra un diagrama con la estructura de la solución **WatchGuard Advanced EPDR**:

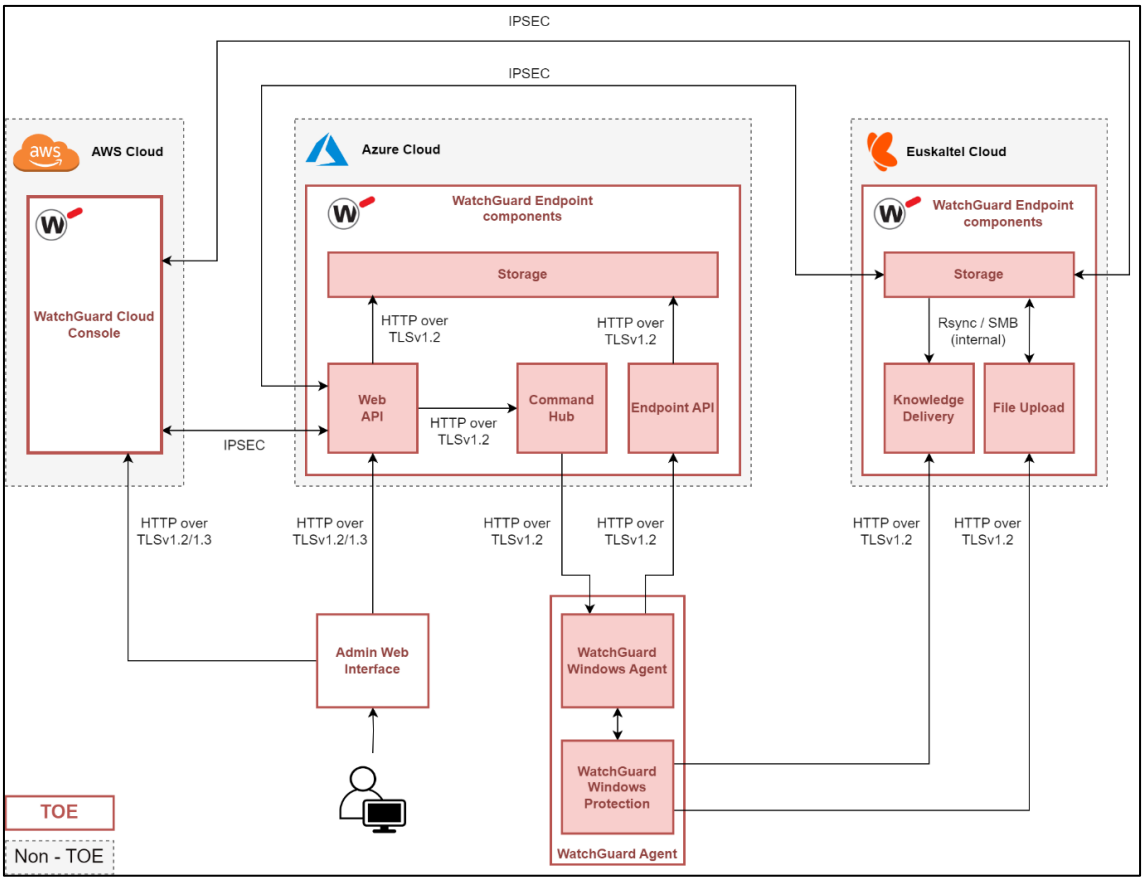


Ilustración 1 Estructura de WatchGuard Advanced EPDR

2 OBJETO Y ALCANCE

El presente documento recoge el Procedimiento de Empleo Seguro de las siguientes soluciones:

a) WatchGuard Advance EPDR (solución base y la mencionada en todo el documento)

b) WatchGuard Endpoint Security Elite

c) WatchGuard EPDR

d) WatchGuard Endpoint Security 360

e) WatchGuard Endpoint Security Prime

Incluyendo los siguientes componentes:

- WatchGuard Advanced EPDR: 4.50.00, 4.70.00 o superior (Cloud Console). La última versión disponible y aplicable para este PES debe consultarse en el Catálogo de CPSTIC [REF3].
- WatchGuard Windows Agent: 1.23.01.0000, 1.25.00.0000 o superior (Management Agent). La última versión disponible y aplicable debe consultarse en el Catálogo de CPSTIC [REF3].
- WatchGuard Windows Protection 8.00.24.0001 o superior (Protection Agent). La última versión disponible y aplicable debe consultarse en el Catálogo de CPSTIC [REF3].

Esta solución ha sido incluida en el CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF3].

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Para garantizar la entrega segura de la solución **WatchGuard Advanced EPDR**, es fundamental seguir un procedimiento detallado que asegure la integridad y autenticidad del software recibido, el cual está definido en la sección "*Endpoint Security > Get Started with WatchGuard Endpoint Security > Endpoint Security Installation Plan*" de las guías REF1.

Para esta cualificación se considera la instalación de estos agentes en equipos con sistema operativo Windows, según viene especificado en la subsección "*Endpoint Security > Get Started with WatchGuard Endpoint Security > Install the Endpoint Software > Install the Endpoint Software Locally > Install the Endpoint Security Software on Windows Computers and Servers*" de REF1.

El resto de los componentes de la nube de WatchGuard son accesibles cuando se activa la cuenta de WatchGuard y la licencia de producto para la solución mencionada. Este proceso se explica en detalle en la sección 4.3 REGISTRO Y LICENCIAS.

4.2 ENTORNO DE INSTALACIÓN SEGURO

Para garantizar un entorno de instalación seguro de los componentes on premise de la solución WatchGuard Advanced EPDR en equipos con sistema operativo Windows, será esencial seguir las precauciones mencionadas a continuación. Adicionalmente, cabe destacar que los componentes en la nube están alojados en la arquitectura de WatchGuard, por lo que el usuario final no necesita realizar ningún despliegue o configuración.

Para la solución cualificada, se considera que los componentes agentes de la solución se instalen en equipos con Windows 11 Professional, siendo también compatibles con sistemas operativos posteriores y anteriores, entre los que se incluye Windows 11 Home y Windows 10 Pro y Home, tal y como se especifica en la sección "*Endpoint Security > Get Started with WatchGuard Endpoint Security > Installation Requirements*" de la guía REF1. Los requerimientos necesarios para estos equipos con este sistema operativo son los siguientes:

- **Requisitos de sistema**: Los equipos finales tendrán instalado Windows 11 Professional con al menos 650 MB de espacio libre para instalar el agente de WatchGuard.
- **Requisitos de privilegios**: La instalación de los agentes precisará de un usuario Windows con privilegios de administrador.
- **Requisitos de red**: Los agentes requieren acceso a múltiples recursos en la nube, por lo que deberán tener acceso a los puertos 80 y 443.

4.3 REGISTRO Y LICENCIAS

El procedimiento de **activación de licencias** para la solución WatchGuard Advanced EPDR viene especificado en la sección "*Endpoint Security > Get Started with WatchGuard Endpoint Security*" de las guías REF1.

4.4 CONSIDERACIONES PREVIAS

Es preciso **configurar las cipher suites** de los canales de comunicación que establezcan los componentes on-premise con los componentes cloud de la solución WatchGuard Advanced EPDR. Se recomienda aplicar esta configuración a nivel de sistema operativo para garantizar el cumplimiento de las cipher suites aceptadas según la guía CCN-STIC-807 para la categoría ALTA del ENS [REF2].

a) En el editor de directivas de grupo local, acceder a "Administrative Templates > Network > SSL Configuration Setting".

b) Hacer clic en "*SSL Cipher Suite Order*" y establecer un listado de las aceptadas por las recomendaciones de las guías CCN, como se indica a continuación: "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256".

c) Para limitar las curvas elípticas ofrecidas, hacer doble clic en "*ECC Curve Order*", habilitarlo e introducir el siguiente texto: "brainpoolP256r1,brainpoolP384r1,brainpoolP512r1,secP256r1,secP384r1,secP521r1".

d) Hacer clic en el botón "*Apply*" y reiniciar el equipo para que las configuraciones se apliquen correctamente.

Nota: Se puede hacer uso de cualquier otra cipher suite o curva recomendada por la guía CCN-STIC-807.

Para el correcto funcionamiento, es necesario que los **equipos finales tengan conectividad** a las siguientes URLs:

- wes-cpp-fulg.pandasecurity.com
- wes-cpp-fusm.pandasecurity.com
- wes-cpp-kw.pandasecurity.com
- endpointgw.aether.deu.pandasecurity.com
- endpointpgw.aether.deu.pandasecurity.com
- wg.cloud.threatseeker.com
- gateway.aether.deu.pandasecurity.com
- commandhubws.aether.deu.pandasecurity.com
- repository.pandasecurity.com
- accesscontrolgw.aether.deu.pandasecurity.com

También es preciso que tengan los siguientes **puertos operativos**:

- Puerto 80 (HTTP)
- Puerto 443 (HTTPS)

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

El entorno operacional por el que está formada la solución cualificada, y que permite dar soporte a sus funcionalidades de seguridad, se detalla a continuación:

- **Usuarios autorizados**. Son los usuarios que acceden y gestionan las funcionalidades de seguridad de la solución cualificada. Para ello, acceden y se autentican en la **WatchGuard Cloud Console** a través de la interfaz de administración. Se recomienda

acceder a esta interfaz a través de un navegador donde las cipher suites y curvas elípticas estén aceptadas para categoría ALTA de ENS según la guía CCN-STIC-807 para proporcionar comunicaciones TLS v1.2 y v1.3 seguras.

- **Dispositivos finales**: Representan los equipos Windows 10 Professional donde el WatchGuard Agent se despliega e instala. Estos equipos deben cumplir las consideraciones mencionadas en la sección 4.2 ENTORNO DE INSTALACIÓN SEGURO.
- **Nube de AWS**: El componente WatchGuard Cloud Console se despliega en la nube de Amazon Web Services, certificada según el ENS con certificado de categoría ALTA.
- **Nube de Azure**: Los componentes de WatchGuard Endpoint utilizados por los usuarios autorizados para gestión de los Agentes WatchGuard, sincronización y recuperación de información de detección, están desplegados sobre entorno cloud de Azure, los cuales están certificados según el ENS con certificado de categoría ALTA.
- **Nube de Euskaltel**: Los componentes de WatchGuard Endpoint utilizados por los Agentes WatchGuard para la clasificación de firmas y carga de ficheros, están desplegados sobre entornos Cloud de Euskaltel, los cuales están certificados según el ENS con certificado de categoría ALTA.

En la siguiente imagen se pueden observar cómo están situados los componentes del entorno de acuerdo con la arquitectura operacional de la solución cualificada:

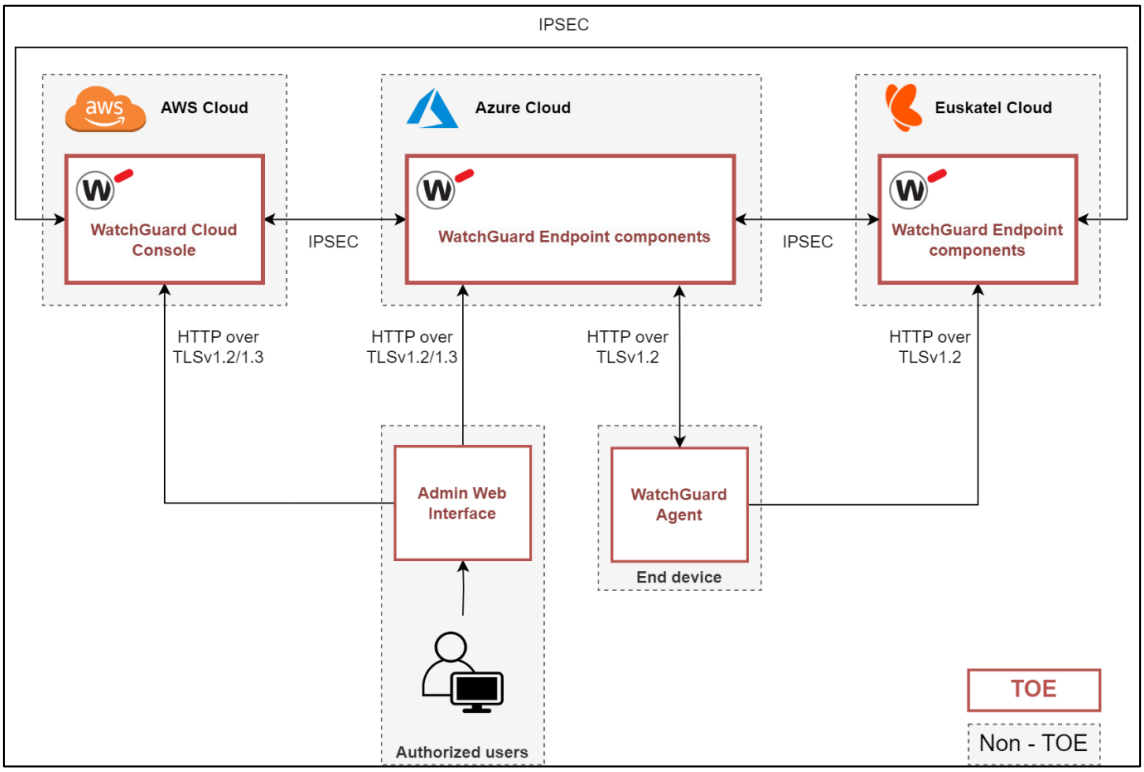


Ilustración 2 Entorno operacional de WatchGuard Advanced EPDR

5 FASE DE INSTALACIÓN

El proceso de instalación de WatchGuard Advanced EPDR consta de una serie de pasos que dependen del estado de la red en el momento de la instalación y del número de equipos y dispositivos que se desean proteger. Se recomienda seguir los pasos definidos en la sección "*Endpoint Security > Get Started with WatchGuard Endpoint Security > Installation Plan*" de REF1. Cabe destacar que, dentro de los pasos definidos en esta sección, la solución cualificada no hará uso de los módulos adicionales mencionados en el paso 2, ni requerirá la habilitación de un proxy, tal y como se indica en el paso 3.

Los WatchGuard Agents deben instalarse siguiendo el plan de instalación definido en la sección "*Endpoint Security > Get Started with WatchGuard Endpoint Security > Installation Plan*" de REF1. En concreto, para la solución cualificada, la estrategia de despliegue utilizada en el paso 4 consistirá en "*Install the Endpoint Security Software locally on Windows computers and Servers*".

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Los componentes WatchGuard Cloud Console y WatchGuard Endpoint han sido evaluados con su configuración por defecto. Los componentes de WatchGuard Endpoint hacen uso de https://deu.cloud.watchguard.com/ para proporcionar acceso a los usuarios que gestionen esta solución.

Nota: Para la interfaz de login de usuarios autorizados, el servicio cualificado redirigirá a estos usuarios a https://wglogin.b2clogin.com, que forma parte de la solución cualificada.

Las cuentas de usuario tendrán una suscripción *tier-2*, la cual define roles específicos para la gestión de las funcionalidades de seguridad de la solución cualificada.

Las siguientes configuraciones deben estar habilitadas en la WatchGuard Cloud Console, en la sección "*Configurar > Endpoints*":

a) En la sección "*GENERAL*":
   i. "Ajustes por equipo":
      a. "Preferencias" > "Mostrar icono en la bandeja del sistema"
      b. "Seguridad frente a manipulaciones no deseadas de las protecciones":
         i. "Solicitar contraseña para desinstalar la protección desde los equipos"
         ii. "Activar protección anti-tamper (impide que los usuarios o ciertos tipos de malware puedan detener las protecciones)"
   ii. "Mis alertas":
      a. "Equipos con error en la protección"
      b. "Equipos sin licencia"
      c. "Errores durante la instalación"
      d. "Equipos no administrados descubiertos"

b) En la sección "*SEGURIDAD*":
   i. "Estaciones y servidores" > "Configuración por defecto":
      a. "General"
         i. "Mostrar alertas de malware, firewall y control de dispositivos"
         ii. "Actualizaciones automáticas de conocimiento"
      b. "Protección avanzada"
         i. "Protección avanzada"
         ii. "Comportamiento: Modo de funcionamiento (Sólo Windows)" > Hardening
         iii. "Anti-exploit: Modo de funcionamiento (Sólo Windows)" > Bloquear
         iv. "Protección contra ataques de red"
         v. "Protección contra ataques de red: Modo de funcionamiento (Sólo Windows)" > Bloquear

vi. "Recoger y mostrar en la consola el usuario que tiene la sesión iniciada en el momento en el que se detectan las amenazas en los equipos"

c. "Antivirus"

i. "Antivirus de archivos"

ii. "Detectar virus"

iii. "Detectar herramientas de hacking y PUPs"

iv. "Bloquear acciones peligrosas"

v. "Crear Decoy Files para ayudar a la detección de ransomware"

ii. "*Indicadores de ataque (IOA)*" > Activar todos los valores de indicadores de ataque.

Por último, la autenticación MFA se aplicará a todos los usuarios asociados a la cuenta a través de la sección "*Administración > Cuenta > Operadores y Roles*". Para ello, haga clic en los tres puntos cerca del nombre del usuario y seleccione la opción "*Activar MFA*".

6.2 AUTENTICACIÓN

La solución WatchGuard Advanced EPDR implementa mecanismos AAA para conceder acceso a la consola web y condicionado a las credenciales suministradas por el administrador de la seguridad del sistema.

La fase de autenticación abarca los procesos que validan las credenciales suministradas y permiten el acceso a la consola de WatchGuard Advanced EPDR. Se implementan dos modos de autenticación:

- Autenticación básica.
- Autenticación de dos factores (2FA).

6.2.1 AUTENTICACIÓN BÁSICA

La autenticación básica de usuarios en la consola web de la solución cualificada consta de credenciales basadas en usuario y contraseña.

Para crear una cuenta de acceso a la consola web con autenticación básica, es necesario utilizar una cuenta con el rol "Administrator" asignado. Tras esto, será preciso seguir los siguientes pasos:

a) Acceder al menú "*Administración*" y, posteriormente, a la sección "*Operadores y Roles*".

b) Hacer clic en el botón "*Añadir Operador*" y completar los siguientes campos: **Nombre de usuario**, **Correo electrónico**, **Nombre**, **Apellidos** y **Seleccionar Rol**. Adicionalmente, habilitar la **Autenticación Multifactor (MFA)** antes de hacer clic en el botón "*GUARDAR*".

6.2.2 AUTENTICACIÓN DE DOS FACTORES

La autenticación de doble factor ocurre en el momento en que un usuario ha introducido sus credenciales de acceso a la consola web.

Si el usuario ha sido creado siguiendo los pasos definidos en la sección 6.2.1 AUTENTICACIÓN BÁSICA, recibirá en su correo electrónico dos correos electrónicos. El primero de ellos es el

correo de activación de la cuenta, pedirá al usuario crear una nueva contraseña que cumpla con los criterios de CCN.

Tras crear la cuenta de usuario, recibirá el segundo correo para configurar la autenticación multifactor a través de la aplicación móvil AuthPoint. La propia página web mostrará los pasos de configuración y de activación de este 2FA.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

La administración de la solución cualificada se realiza de forma remota en la consola web a través de la interfaz de administración. Esta comunicación se realiza a través de HTTPS (HTTP sobre TLS v1.2 o superior) haciendo uso de ciphersuites aceptadas por la guía CCN-STIC-807 para categoría ALTA de ENS.

La administración remota a través de esta consola permite a los usuarios autorizados ejercer las siguientes funcionalidades de seguridad:

- Gestión de usuarios, permisos y doble factor de autenticación (2FA).
- Gestión de políticas de dispositivos finales.
- Gestión de las políticas de detección y respuesta.
- Gestión del nivel de riesgo asociado a la detección.
- Gestión de alertas y emails.

Se deben considerar las recomendaciones de configuración a nivel de sistema operativo, definidas en la sección 4.4 CONSIDERACIONES PREVIAS, para limitar las ciphersuites a nivel de cliente y cumplir con las guías CCN.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

La solución WatchGuard Advanced EPDR define roles de usuario para poder administrar las funcionalidades de seguridad que ofrece. Esta gestión viene definida en la sección "*WatchGuard Account Help > Manage WatchGuard Users > Manage WatchGuard Cloud Operators*" de REF1.

Por defecto, en la creación de la cuenta de un usuario, la contraseña que se solicita cumple con las recomendaciones de las guías CCN:

- Longitud mínima de 12 caracteres.
- La contraseña debe estar compuesta de letras mayúsculas, letras minúsculas, números y símbolos especiales.

No se requiere otra configuración adicional para los administradores más allá de la gestión definida a través de los manuales de la solución cualificada.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Para acceder a la consola web, la comunicación se realizará a través del puerto 443 con la última versión de un navegador compatible.

Por defecto, los WatchGuard Agents instalados en los equipos finales se conectan a los componentes nube de WatchGuard Endpoint definidos en la sección 4.4 CONSIDERACIONES PREVIAS.

6.5 GESTIÓN DE CERTIFICADOS

Los usuarios finales que se beneficien del uso del servicio WatchGuard Endpoint Advanced EPDR no precisan de configuración de certificados digitales, ya que estos se encuentran preconfigurados y gestionados por defecto por WatchGuard para los distintos endpoints de la solución. Dichos certificados, firmados con claves **RSA de 3072 bits** o superiores, se emplean para la autenticación de los canales de comunicación a la consola web para ejercer funcionalidades de seguridad entre componentes de la solución o con componentes del entorno operacional.

6.6 SERVIDORES DE AUTENTICACIÓN

La solución cualificada no hace uso de servidores externos de autenticación. La autenticación y autorización de usuarios la realiza el servicio de WatchGuard a través de las credenciales de usuario y el doble factor de autenticación (2FA).

6.7 SINCRONIZACIÓN

Se recomienda que todos los equipos protegidos por los agentes de WatchGuard mantengan una sincronización precisa de fecha y hora del sistema operativo.

Una hora del sistema correctamente sincronizada es fundamental para el correcto funcionamiento de los registros de eventos, la correlación de alertas, la validez de certificados digitales y la trazabilidad de las acciones de seguridad. Por ello, se recomienda que los sistemas operativos donde se instalen los agentes de WatchGuard estén configurados para sincronizar su reloj mediante servicios NTP confiables, como los proporcionados por el sistema operativo o por servidores internos de la organización. Aunque el producto no implementa autenticación NTP propia, se sugiere, siempre que sea posible, utilizar servidores NTP que soporten autenticación para reforzar la integridad de la sincronización horaria.

6.8 ACTUALIZACIONES

El procedimiento de actualización viene definido en la sección "*Endpoint Security > Get Started with WatchGuard Endpoint Security > Upgrade Process*" de REF1.

Los componentes de la solución alojados en la nube son actualizados conforme surgen parches de seguridad que implementa WatchGuard.

Respecto a los agentes, el administrador debe verificar la integridad de las actualizaciones mediante la comprobación de un hash SHA-256 previo a la instalación. Estas actualizaciones solo se realizarán si el administrador lo define en la consola web.

6.9 AUTO-CHEQUEOS

La solución WatchGuard Advanced EPDR no implementa mecanismos automáticos de auto-chequeo (self-test) para verificar la integridad del software.

A pesar de no contar con auto-chequeos, los agentes de WatchGuard aplican medidas de seguridad que refuerzan su integridad y resistencia frente a manipulaciones. En particular, el agente no solicita la asignación de direcciones de memoria explícitas del sistema ni asigna

memoria con permisos simultáneos de escritura y ejecución. Además, está configurado por defecto con permisos de archivo que impiden accesos no autorizados.

6.10 ALTA DISPONIBILIDAD

La solución **WatchGuard Advanced EPDR** se apoya en una arquitectura distribuida en entornos cloud de alta disponibilidad, desplegada en plataformas como **AWS**, **Microsoft Azure** y **Euskaltel**. Estas infraestructuras proporcionan mecanismos nativos de redundancia, tolerancia a fallos y escalabilidad automática, lo que garantiza la continuidad del servicio incluso ante incidencias en uno de los entornos. Aunque no se requiere configuración específica por parte del usuario final, estas plataformas aseguran que los servicios alojados mantengan una operatividad constante y segura.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

La plataforma de WatchGuard permite un registro de auditoría de las acciones llevadas a cabo por los componentes de la solución y sus servicios, además de los registros de login de los usuarios. La sección "*WatchGuard Cloud Platform > Alerts, Notifications, and Reports > See Audit Logs*" de REF1 contiene información sobre estos registros de auditoría.

A modo de ejemplo, la solución cualificada registra los siguientes eventos:

- Login y logout de usuarios registrados.
- Cambios en las credenciales de usuarios.
- Cambios en el servicio, incluyendo gestión de usuarios, dispositivos finales y políticas de detección y/o respuesta.
- Gestión del nivel de riesgo asociado con la detección.
- Gestión de alertas.

6.11.2 ALMACENAMIENTO LOCAL

La solución WatchGuard Advanced EPDR no realiza almacenamiento local de registros de auditoría en sus agentes, ya que toda la información generada por estos se transmite y almacena de forma centralizada en la infraestructura cloud de WatchGuard.

Esta arquitectura permite una gestión unificada, segura y resiliente de los registros, eliminando la necesidad de configuración adicional por parte del usuario para el almacenamiento local. Por tanto, no se requiere ninguna acción específica para garantizar la seguridad del almacenamiento de registros en los equipos protegidos.

6.11.3 ALMACENAMIENTO REMOTO

La solución WatchGuard Advanced EPDR no requiere configuración para el envío de registros a servidores remotos tipo syslog, ya que todos los eventos y datos de auditoría generados por los agentes se almacenan de forma centralizada en la infraestructura cloud de WatchGuard.

Esta infraestructura está desplegada en plataformas que cumplen con los requisitos del ENS en categoría alta, incluyendo Microsoft Azure, AWS y Euskaltel, lo que garantiza un almacenamiento remoto seguro, con mecanismos de cifrado, redundancia y acceso controlado.

Por tanto, no es necesario configurar protocolos adicionales como TLS o IPsec para el envío de registros por parte del usuario final.

6.12 BACKUP

En la solución WatchGuard Advanced EPDR, las configuraciones, registros de actividad y otra información crítica generada por los agentes se almacenan de forma centralizada en la infraestructura cloud de WatchGuard. Esta infraestructura utiliza buckets S3 de Amazon Web Services (AWS) como sistema de almacenamiento principal, con mecanismos de replicación automática que garantizan la disponibilidad y resiliencia de los datos.

Aunque el usuario final no necesita realizar configuraciones manuales de backup, se recomienda verificar periódicamente desde la consola de administración que los datos se están sincronizando correctamente. La realización de copias de seguridad adicionales por parte del cliente no es necesaria, ya que el sistema está diseñado para garantizar la persistencia y recuperación de la información conforme a las buenas prácticas de seguridad en la nube.

7 REFERENCIAS

[REF1] Manuales de configuración y administración de WatchGuard Advanced EPDR

[REF2] Guía de Seguridad de las TIC CCN-STIC 807 - Criptología de empleo en el Esquema Nacional de Seguridad, Mayo 2022

[REF3] CPSTIC

8 ABREVIATURAS

2FA	Two-Factor Authentication
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
API	Application Programming Interface
AWS	Amazon Web Services
CCN	Centro Criptológico Nacional
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
ENS	Esquema Nacional de Seguridad.
EPDR	Endpoint Protection Detection and Response
EPP	Endpoint Protection Platform
GCM	Galois/Counter Mode
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over TLS
IOA	Indicator of Attack
MB	Megabyte
MFA	Multifactor Authentication
NIPO	Número de Identificación de Publicaciones Oficiales
NTP	Network Time Protocol
PUP	Potentially Unwanted Program
RSA	Rivest–Shamir–Adleman algorithm
S3	Simple Storage Service (de AWS)
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones
TLS	Transport Layer Security
URL	Uniform Resource Locator
WG	WatchGuard