Guía de Seguridad de las TIC
CCN-STIC 1244

Procedimiento de Empleo Seguro
Panda Adaptive Defense 360 / Cytomic 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 14:07:00 +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
1.1 PANDA ADAPTIVE DEFENSE 360 Y CYTOMIC ADVANCED EPDR 3
1.2 PLATAFORMA AETHER Y PLATAFORMA CYTOMIC 3
2 OBJETO Y ALCANCE 3
3 ORGANIZACIÓN DEL DOCUMENTO 4
4 FASE PREVIA A LA INSTALACIÓN 5
4.1 ENTREGA SEGURA DEL PRODUCTO 5
4.2 ENTORNO DE INSTALACIÓN SEGURO 5
4.3 REGISTRO Y LICENCIAS 5
4.4 CONSIDERACIONES PREVIAS 5
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 6
5 FASE DE INSTALACIÓN 8
6 FASE DE CONFIGURACIÓN 9
6.1 MODO DE OPERACIÓN SEGURO 9
6.2 AUTENTICACIÓN 10
6.2.1 AUTENTICACIÓN BÁSICA 10
6.2.2 AUTENTICACIÓN DE DOS FACTORES 11
6.3 ADMINISTRACIÓN DEL PRODUCTO 11
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 11
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 11
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 12
6.5 GESTIÓN DE CERTIFICADOS 12
6.6 SERVIDORES DE AUTENTICACIÓN 12
6.7 SINCRONIZACIÓN 12
6.8 ACTUALIZACIONES 12
6.9 AUTO-CHEQUEOS 13
6.10 ALTA DISPONIBILIDAD 13
6.11 AUDITORÍA 13
6.11.1 REGISTRO DE EVENTOS 13
6.11.2 ALMACENAMIENTO LOCAL 13
6.11.3 ALMACENAMIENTO REMOTO 14
6.12 BACKUP 14
7 REFERENCIAS 15
8 ABREVIATURAS 16

1 INTRODUCCIÓN

Panda Adaptive Defense 360 y **Cytomic Advanced EPDR** son dos servicios gestionados que protegen los equipos informáticos de las empresas, acotan el alcance de los problemas de seguridad encontrados y ayudan a establecer planes de respuesta y prevención frente a las amenazas desconocidas y a los ataques dirigidos avanzados (APTs).

Panda Adaptive Defense 360 está dividido en dos áreas funcionales bien diferenciadas:

a) Panda Adaptive Defense 360

b) Plataforma Aether

Cytomic Advanced EPDR está dividido en dos áreas funcionales bien diferenciadas:

a) Advanced EPDR

b) Plataforma Cytomic

1.1 PANDA ADAPTIVE DEFENSE 360 Y CYTOMIC ADVANCED EPDR

Son los productos que implementan todas las características orientadas a garantizar la seguridad de los puestos de usuario y los servidores, sin requerir la intervención del administrador de la red.

1.2 PLATAFORMA AETHER Y PLATAFORMA CYTOMIC

Son los dos ecosistemas donde se ejecutan los productos de Panda Security y Advanced EPDR. Estas plataformas entregan en tiempo real, de forma ordenada y con un gran nivel de detalle, toda la información generada por cada solución sobre los procesos, los programas ejecutados por los usuarios y los dispositivos que pertenecen a la infraestructura IT de las organizaciones.

Estas plataformas son eficientes, extensibles, escalables y están diseñadas para cubrir las necesidades de las grandes cuentas y de los MSPs.

2 OBJETO Y ALCANCE

El presente documento recoge el Procedimiento de Empleo Seguro de las soluciones **Panda Adaptive Defense 360** y **Cytomic Advanced EPDR**, incluyendo los siguientes componentes:

a) Panda Adaptive Defense 360: 4.50.00 (Cloud Console)

b) Cytomic Advanced EPDR: 4.50.00 (Cloud Console)

c) Windows Agent: 1.23.01.0000 (Management Agent)

d) Windows Protection: 8.00.24.0001 (Protection Agent)

Ambas soluciones han sido incluidas en el Catálogo de Productos (CPSTIC), para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF4].

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 las soluciones **Panda Adaptive Defense 360** y **Cytomic Advanced EPDR**, es fundamental seguir un procedimiento detallado que asegure la integridad y autenticidad del software recibido. Para esta cualificación se considera la instalación de los agentes en equipos con sistema operativo Windows, según viene especificado en la sección "*Instalación del software cliente > Instalación en sistemas Windows*" de las guías [REF1] y [REF2].

El resto de los componentes de la nube son accesibles cuando se activa la cuenta de usuario y la licencia del producto. 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 las soluciones **Panda Adaptive Defense 360** y **Cytomic 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 plataforma de Aether o Cytomic, por lo que el usuario final no necesita realizar ningún despliegue o configuración.

Los requisitos de instalación de los componentes software vienen especificados en la sección "*Instalación del software cliente > Instalación en sistemas Windows > Requisitos de instalación*" de las guías [REF1] y [REF2].

Para las soluciones cualificadas, se considera que los componentes agentes se instalen en equipos con Windows 11 Professional, tal y como se especifica en la sección "*Funcionalidades del producto y requisitos > Requisitos de plataformas Windows > Sistemas operativos soportados*" de las guías [REF1] y [REF2].

4.3 REGISTRO Y LICENCIAS

El procedimiento de **activación de licencias** para las soluciones **Panda Adaptive Defense 360** y **Cytomic Advanced EPDR** viene especificado en la sección "*Licencias*" de las guías [REF1] y [REF2].

La gestión de las cuentas de usuario está definida en la sección "*Acceso, control y supervisión de la consola de administración > Gestión de cuentas de usuario*" de las guías [REF1] y [REF2].

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 las soluciones **Panda Adaptive Defense 360** y **Cytomic 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 [REF3] para la categoría ALTA del ENS.

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

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 [REF3].

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

a) wes-cpp-fulg.pandasecurity.com
b) wes-cpp-fusm.pandasecurity.com
c) wes-cpp-kw.pandasecurity.com
d) endpointgw.aether.deu.pandasecurity.com
e) endpointpgw.aether.deu.pandasecurity.com
f) wg.cloud.threatseeker.com
g) gateway.aether.deu.pandasecurity.com
h) commandhubws.aether.deu.pandasecurity.com
i) repository.pandasecurity.com
j) accesscontrolgw.aether.deu.pandasecurity.com

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

a) Puerto 80 (HTTP)
b) Puerto 443 (HTTPS)

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

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

a) **Usuarios autorizados:** Son los usuarios que acceden y gestionan las funcionalidades de seguridad de la solución cualificada. Para ello, acceden y se autentican en cada consola web. Se recomienda acceder a esta interfaz a través de un navegador donde las cipher suites y curvas elípticas estén aceptadas para la categoría ALTA de ENS según la guía CCN-STIC-807 [REF3] para proporcionar comunicaciones TLS v1.2 y v1.3 seguras.

b) **Dispositivos finales**: Representan los equipos Windows 11 Professional en los que el agente se despliega e instala. Estos equipos deben cumplir las consideraciones mencionadas en la sección 4.2 ENTORNO DE INSTALACIÓN SEGURO**.**

c) **Nube de AWS:** La consola web se despliega en la nube de Amazon Web Services, certificada según el ENS con categoría ALTA.

d) **Nube de Azure:** Los componentes de **Panda Adaptive Defense 360** y **Cytomic Advanced EPDR** utilizados por los usuarios autorizados para gestión de los agentes, sincronización y recuperación de información de detección, están desplegados

sobre el entorno cloud de Azure, el cual está certificado según el ENS con categoría ALTA.

e) **Nube de Euskaltel:** Los componentes de **Panda Adaptive Defense 360 y Cytomic Advanced EPDR** utilizados por los agentes para la clasificación de firmas y la carga de ficheros están desplegados sobre entornos cloud de Euskaltel, los cuales están certificados según el ENS con categoría ALTA.

5 FASE DE INSTALACIÓN

El proceso de instalación para **Panda Adaptive Defense 360** y **Cytomic 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 "*Instalación del software cliente > Instalación en sistemas Windows > Integración de equipos según su dirección IP*" de [REF1] y [REF2].

Los agentes deben instalarse siguiendo el plan de instalación definido en la sección "*Instalación del software cliente > Instalación en sistemas Windows > Instalación del paquete descargado*" de las guías [REF1] y [REF2].

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Los componentes de la solución **Panda Adaptive Defense 360** han sido evaluados partiendo de su configuración por defecto, a la cual se le han aplicado las configuraciones mencionadas en este documento. Los usuarios pueden hacer uso de la consola web alojada en https://wg.aether.pandasecurity.com/ para gestionar esta solución.

Los componentes de la solución **Cytomic Advanced EPDR**, del mismo modo, han sido evaluados partiendo de su configuración por defecto, a la cual se le han aplicado las configuraciones mencionadas en este documento. Los usuarios pueden hacer uso de la consola web alojada en https://manage.cytomicmodel.com/ para gestionar esta solución.

Las siguientes configuraciones deben estar habilitadas en la consola web, en la sección "*Configuración*":

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 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 debe ser aplicada a todos los usuarios asociados a la cuenta a través de la sección "*Configuración > General > Usuarios > Seguridad*" y seleccionar la opción "*Requerir verificación en dos pasos*".

6.2 AUTENTICACIÓN

Las soluciones **Panda Adaptive Defense 360** y **Cytomic Advanced EPDR** implementan mecanismos AAA para conceder acceso a sus consolas web, 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 cada consola web. Se implementan dos modos de autenticación:

a) Autenticación básica.

b) Autenticación de dos factores (2FA).

6.2.1 AUTENTICACIÓN BÁSICA

La autenticación básica de usuarios en la consola web de cada una de las soluciones cualificadas consta de credenciales basadas en usuario y contraseña.

Para crear la primera cuenta de usuario que permita gestionar cada solución cualificada, es preciso seguir los pasos definidos en la sección "*Acceso, control y supervisión de la consola de administración > Gestión de cuentas de usuario > Crear la primera cuenta de usuario para clientes de Panda Security*" de [REF1] y "*Acceso, control y supervisión de la consola de administración > Gestión de cuentas de usuario > Crear la primera cuenta de usuario*" de [REF2].

Para crear una cuenta de acceso a las consolas web con autenticación básica, es necesario utilizar una cuenta con el rol "*Control total*" asignado. Tras esto, será preciso seguir los siguientes pasos:

a) Acceder al menú "*Configuración*" y, posteriormente, a la sección "*General > Usuarios*".

b) Cuando se haga clic en el botón "*Añadir*", completar el campo "*Email de Acceso*" y seleccionar el rol 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 en cada consola web a la que accede.

Si el usuario ha sido creado siguiendo los pasos definidos en la sección 6.2.1 AUTENTICACIÓN BÁSICA, recibirá dos correos electrónicos, donde el correo de activación de cuenta le pedirá al usuario que cree una nueva contraseña que cumpla con los criterios de CCN.

Tras crear la cuenta de usuario, recibirá un 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 las soluciones cualificadas se realiza de forma remota en cada 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 [REF3] para la categoría ALTA del ENS.

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

a) Gestión de usuarios, permisos y autenticación de dos factores (2FA).
b) Gestión de políticas de dispositivos finales.
c) Gestión de las políticas de detección y respuesta.
d) Gestión del nivel de riesgo asociado a la detección.
e) Gestión de alertas y correos electrónicos.

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 del CCN.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

Las soluciones **Panda Adaptive Defense 360** y **Cytomic Advanced EPDR** definen roles de usuario para poder administrar las funcionalidades de seguridad que ofrecen. Esta gestión viene definida en la sección "*Acceso, control y supervisión de la consola de administración > Gestión de roles y permisos*" de [REF1] y [REF2].

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

a) Longitud mínima de 12 caracteres.
b) 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 [REF1] y [REF2].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Para acceder a cada una de las consolas web, la comunicación se debe realizar a través del puerto 443 (https) utilizando la última versión de un navegador compatible.

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

6.5 GESTIÓN DE CERTIFICADOS

Los usuarios finales que se beneficien del uso del servicio **Panda Adaptive Defense 360** y **Cytomic Advanced EPDR** no precisan configuración de certificados digitales, ya que estos se encuentran preconfigurados y gestionados por el fabricante 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 hacia cada consola web y para proporcionar funcionalidades de seguridad entre componentes de la solución o con componentes del entorno operativo.

6.6 SERVIDORES DE AUTENTICACIÓN

Las soluciones cualificadas no hacen uso de servidores externos de autenticación. La autenticación y autorización de usuarios se realizan 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 Panda Adaptive Defense 360** y **Cytomic Advanced EPDR** 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 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 "*Actualización del producto*" de [REF1] y [REF2].

Los componentes de la solución alojados en la nube son actualizados conforme surgen parches de seguridad que implementan el propio fabricante.

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 de cada solución.

La obtención de este hash se puede realizar conforme a los pasos especificados en la sección "Configuración de software autorizado > Configuración de Software autorizado > Opciones de configuración del módulo Software autorizado > Calcular el MD5 o SHA-256 de uno o más ficheros" de los manuales [REF1] y [REF2].

6.9 AUTO-CHEQUEOS

Las soluciones **Panda Adaptive Defense 360** y **Cytomic Advanced EPDR** no implementan mecanismos automáticos de auto-chequeo (self-test) para verificar la integridad del software.

A pesar de no contar con auto-chequeos, los agentes aplican medidas de seguridad que refuerzan su integridad y resistencia frente a manipulaciones. En particular, los agentes no solicitan la asignación de direcciones de memoria explícitas del sistema ni asignan memoria con permisos simultáneos de escritura y ejecución. Además, están configurados por defecto con permisos de archivo que impiden accesos no autorizados.

6.10 ALTA DISPONIBILIDAD

Las soluciones **Panda Adaptive Defense 360** y **Cytomic Advanced EPDR** se apoyan 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

Las plataformas de Aether y Cytomic permiten un registro de auditoría de las acciones llevadas a cabo por los componentes de la solución y sus servicios, además de los registros de inicio de sesión de los usuarios. La sección "*Acceso, control y supervisión de la consola de administración > Registro de la actividad de las cuentas de usuario*" de [REF1] y [REF2] contiene información sobre estos registros de auditoría.

A modo de ejemplo, las soluciones cualificadas registran los siguientes eventos:

a) Inicio y cierre de sesión de usuarios registrados.
b) Cambios en las credenciales de los usuarios.
c) Cambios en el servicio, incluyendo la gestión de usuarios, dispositivos finales y políticas de detección y/o respuesta.
d) Gestión del nivel de riesgo asociado a la detección.
e) Gestión de alertas.

6.11.2 ALMACENAMIENTO LOCAL

Las soluciones **Panda Adaptive Defense 360** y **Cytomic Advanced EPDR** no realizan 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 Aether y Cytomic.

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

Las soluciones **Panda Adaptive Defense 360** y **Cytomic Advanced EPDR** no requieren 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 Aether y Cytomic.

Esta infraestructura está desplegada en plataformas que cumplen con los requisitos del ENS en categoría ALTA, incluyendo Google Cloud, 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 las soluciones **Panda Adaptive Defense 360** y **Cytomic 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 Aether y Cytomic. 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.

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] Guía de administración de Panda Adaptive Defense 360, version 4.60.00

[REF2] Guía de administración de Advanced EPDR, version 4.60.00

[REF3] Guía de Seguridad de las TIC CCN-STIC 807 - Criptología de empleo en el Esquema Nacional de Seguridad, Mayo 2022

[REF4] CPSTIC https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

8 ABREVIATURAS

2FA	Two-Factor Authentication
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
APT	Advanced Persistent Threat
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
IP	Internet Protocol
IPsec	Internet Protocol Security
IT	Information Technology
MFA	Multifactor Authentication
MSP	Managed Service Provider
NTP	Network Time Protocol
PUP	Potentially Unwanted Program
PUPs	Potentially Unwanted Programs
RSA	Rivest–Shamir–Adleman algorithm
S3	Simple Storage Service
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