Guía de Seguridad de las TIC
CCN-STIC 1245

Procedimiento de Empleo Seguro
Devo SIEM

Febrero 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN, ou=SELLO ELECTRONICO, 2.5.4.97=VATES-S2800155J, serialNumber=S2800155J, cn=CCN
2026.02.18 15:51:33 +01'00'

Fecha de Edición: Febrero 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

ÍNDICE

1 INTRODUCCIÓN

1. **Devo** es una plataforma de análisis de datos diseñada para el acceso y análisis de los datos de todo un dominio de una organización, tanto datos de flujo como históricos, en tiempo real y a escala. Se referencia por dominio de una organización al entorno que permite el acceso a diferentes conjuntos y subconjuntos de datos de la organización.
2. Se trata de una herramienta de tipo SIEM (Security Information and Event Management) en la nube. Está formada por distintos componentes, que se detallan a continuación.
3. Devo cuenta con un **Web Portal** para la administración y uso de las capacidades de seguridad de la plataforma que cuenta con un mecanismo de control de acceso en base a roles.
4. El servicio cuenta además con una aplicación software, **Devo Relay**, que se encarga de recibir los eventos y datos de diversas fuentes, los etiqueta y los reenvía a los balanceadores de carga, o **Event Load Balancer (ELB)**.
5. Estos balanceadores se encargan de gestionar las cargas de eventos recibidas en el nodo central, **Meta node**, que los reenviará a los **Data nodes** para procesar las diferentes peticiones de forma jerárquica según han sido categorizados y distribuidos.
6. Los componentes Meta node, Data nodes, ELB y Web Portal se encuentran desplegados en la nube de Devo, mientras que el componente Devo Relay reside instalado en la red interna de la organización.

2 OBJETO Y ALCANCE

7. El presente documento recoge el Procedimiento de Empleo Seguro del servicio **Devo**, incluyendo los siguientes componentes:

    - Devo *Platform* v8.x.x (entorno nube):
        - Web Portal y Backoffice.
        - ELB.
        - Data nodes.
        - Meta nodes.
    - Entorno de la organización:
        - DEVO Relay v2.13.3

8. Esta solución ha sido incluida en el Catálogo de Productos STIC bajo la familia de "**Sistemas de Gestión de Eventos de Seguridad (SIEM)**" correspondiente al Anexo B.6 para categoría ALTA de ENS.

9. El alcance de este documento cubre las recomendaciones de seguridad necesarias para el despliegue y configuración segura del producto en entornos empresariales y organismos públicos.

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 para tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones para 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

10. Para adquirir la suscripción de **Devo**, se debe de acceder al portal de contacto [PORTAL-CONTACTO] y rellenar el formulario correspondiente.
11. Para acceder al portal de inicio de sesión, el usuario administrador debe seguir las indicaciones sobre navegadores web que recomienda [NAVEGADORES-COMPATIBLES].
12. Una vez adquirida la suscripción al servicio, el usuario administrador recibe el enlace de registro al servicio [REGISTRO] y debe iniciar sesión en la página web de Devo [WEB], con sus credenciales de administrador, conformadas por usuario y contraseña.

4.2 ENTORNO DE INSTALACIÓN SEGURO

13. El componente software DEVO Relay debe instalarse en el sistema operativo *Ubuntu* 22 o superior en una máquina virtual que cumpla con los requisitos [REQUISITOS-UBUNTU] descritos por el fabricante, en un entorno físico seguro tipo CPD en el que el acceso se encuentre restringido a personal autorizado.
14. La cualificación contempló el uso de una máquina virtual con los siguientes requisitos mínimos:

Tipo	Requisitos mínimos
Hardware	• 2 CPU • Memoria: 8 GB • La memoria del disco duro debe ser el doble de la memoria intermedia necesaria.
Software	Ubuntu 22 o superior
Red	Para los usuarios de Europa: • Relay API (api-eu.devo.com) • Query API (apiv2-eu.devo.com) Los siguientes puertos deben ser usados exclusivamente por el Relay: • Puertos internos del Relay: 5140 and 12996-12998. • Puertos de entrada reservados: 12999 al 13002 configurados con reglas por defecto. • Puertos de entrada personalizados: 13003 al 13xxx reservados para reglas personalizadas (el número exacto de puertos depende del número de reglas a crear).
Topología	Requisitos de nodo simple: • Una máquina con los requisitos listados arriba.

	• Una dirección IP para el Relay.

Tabla 1: Requisitos mínimos

4.3 REGISTRO Y LICENCIAS

15. Las licencias para el acceso a la plataforma de **Devo** las proporciona el propio fabricante a través del portal de contacto referenciado en la sección 4.1 ENTREGA SEGURA DEL PRODUCTO.

4.4 CONSIDERACIONES PREVIAS

16. Los administradores deben configurar los dispositivos de red de su infraestructura para que envíen los registros de auditoría que se van a analizar al Devo Relay a través del protocolo SYSLOG y HTTPS.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

17. El entorno de operación donde la solución de Devo va a proporcionar su funcionalidad está dividido en dos infraestructuras principales:

    - Infraestructura del cliente (donde se instala el componente Devo Relay).
    - Infraestructura en la nube donde el resto de los componentes de Devo (ELB, nodos, Web Portal, Backoffice) están desplegados.

18. Las entidades principales que participan en la infraestructura del cliente se describen a continuación:

    - **Hosts**. Estas máquinas envían directamente los datos al Devo Relay o a la infraestructura en la nube de Devo.
    - **Relay**. Tiene el componente Devo Relay instalado y es responsable de recolectar todos los datos de las diferentes fuentes configuradas para, posteriormente, enviarlos a la infraestructura en la nube de Devo.
    - **Dispositivos cliente**. Representa cualquier tipo de dispositivo ubicado en la infraestructura del cliente que envía eventos al producto. Estos eventos se envían al Devo Relay antes de enviarse a la infraestructura en la nube de Devo. Se diferencian con los hosts en que los hosts pueden enviar datos tanto al Devo Relay como a los ELB, ya que pueden establecer conexiones HTTPS, en cambio, los dispositivos de cliente no tienen la capacidad de establecer conexiones HTTPS (por ejemplo, una impresora), y por tanto tienen que enviar los datos mediante Syslog al Devo Relay, para que este los envíe a la infraestructura en la nube de Devo.
    - **Proveedor de Identidad externo**. El proveedor externo proporciona a los administradores y usuarios autenticación para acceder al producto a través de la interfaz web. Para realizar esta autenticación, se hace uso de OpenID [OPENID].

19. La agrupación de componentes denominada como Devo *Platform* (infraestructura en la nube) se encuentran desplegados en el entorno AWS.

5 FASE DE INSTALACIÓN

20. El único componente software que se debe de instalar es el componente **Devo *Relay***. La instalación de Devo Relay se realiza únicamente para un solo nodo, siguiendo los pasos descritos en [INSTALACIÓN-DEVO-RELAY].

21. Una vez este componente se ha instalado correctamente, su configuración se puede realizar a través de línea de comandos o interfaz web. Este proceso viene documentado en [CONFIGURACIÓN-DEVO-RELAY].

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

22. La configuración inicial para llegar a un modo de operación seguro es la siguiente:

    a) Para comenzar a hacer uso del servicio, el usuario administrador debe crear un dominio de Devo siguiendo los pasos definidos en [CREACIÓN-DOMINIO].

    b) Para conectar el componente DEVO Relay al dominio creado, se deben seguir los pasos descritos en [CONEXIÓN-DEVO-RELAY].

    c) A continuación, se debe de configurar el componente **ELB**. Este componente cuenta con balanceo para tráfico *syslog* y tráfico HTTPS. Para ambos tráficos, se debe de seguir la [CONFIGURACIÓN-ELB].

    d) Finalmente, se deben configurar las alertas y notificaciones, correspondientes con mensajes generados por el servicio de Devo cuando ocurre un determinado evento en el dominio creado. Para llevar a cabo esta configuración, se deben seguir los pasos descritos en [ALERTAS] para las definiciones de alertas y cómo configurar su activación.

23. La alerta de desviación activa una alerta cada vez que un valor agregado de un único elemento agrupado es significativamente superior o inferior a la mediana. Por lo tanto, para activar esta alerta, es necesario generar suficientes datos para calcular el parámetro de la mediana.

6.2 AUTENTICACIÓN

24. Los mecanismos de autenticación usados por el servicio son los siguientes:

    - **Usuarios administradores.** La autenticación se puede realizar tanto de forma local (integrado en la propia lógica del producto), usando un usuario y contraseña (la cual debe estar configurada con un mínimo de 12 caracteres), como integrando un proveedor de identidad, el cual debe estar listado en el CPSTIC.
    - **Autenticación entre componentes del servicio** mediante certificados X.509.V3 y claves de acceso.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

25. La administración del servicio Devo la realiza un usuario administrador final de forma remota a través del componente **Devo *web portal* (GUI)**. En la configuración cualificada, la comunicación de estos administradores con la interfaz de gestión web se realiza a través de **TLS v1.2 o superior**.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

26. Devo permite gestionar usuarios que puedan ejercer las funcionalidades de seguridad en el portal web de Devo, tal y como se indica en [USUARIOS].

27. Existe una lista de roles de usuario de administración predefinidos [ROLES] y también cómo configurarlos para los usuarios creados. Los roles son un conjunto de permisos, que permiten ejercer unas funcionalidades de seguridad u otras dependiendo del tipo de permiso. Adicionalmente, el usuario administrador puede crear nuevos roles personalizados dependiendo de las funcionalidades que se deseen asignar a dicho rol.
28. Se recomienda que la gestión de las sesiones y procesos de autenticación de usuarios se realice a través del proveedor de identidad configurado mediante OpenID [OPENID].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

29. Para enviar eventos a través de un canal cifrado al Relay, es necesario configurar un servicio de tunelización, denominado stunnel [STUNNEL], instalado en la máquina del componente Devo Relay para que acepte conexiones SSL y, a continuación, reenvíe los datos al Relay.
30. La configuración de puertos de la máquina donde se instala el componente Devo Relay viene definida en la Tabla 1: Requisitos mínimos de la sección 4.2 ENTORNO DE INSTALACIÓN SEGURO.

6.5 GESTIÓN DE CERTIFICADOS

31. Los administradores pueden crear y gestionar los certificados X.509 utilizados para la autenticación de conexiones Syslog con los componentes de Devo.

6.6 SINCRONIZACIÓN

32. Devo ofrece un servicio alojado en la nube de AWS que proporciona la infraestructura necesaria para asegurar que todos los procesos operen con una referencia temporal precisa y consistente.
33. Para ello, los servidores donde los componentes cloud de Devo están alojados y ejecutando su funcionalidad están basados en el protocolo Network Time Protocol (NTP), eliminando la necesidad de configurar por parte del cliente servidores externos de sincronización.
34. Puesto que la sincronización de los componentes de Devo que analizan los eventos se realiza de forma centralizada por AWS, no se requiere intervención de ningún usuario final en este aspecto.
35. Nota: es indispensable que los equipos o dispositivos que generan los datos dispongan de la correcta configuración de fecha y hora.

6.7 ACTUALIZACIONES

36. Las actualizaciones de los componentes de Devo *Platform* son realizadas directamente por el personal administrativo de Devo.
37. Las actualizaciones del componente Devo Relay se deben de realizar siguiendo los pasos declarados en [CONFIGURACIÓN-DEVO-RELAY].

6.8 AUTO-CHEQUEOS

38. Dado que el servicio de Devo SIEM es un SaaS (*Software as a Service*), los auto chequeos y el monitoreo de integridad del sistema se gestionan de manera centralizada por el proprio fabricante. Estos servicios están diseñados para funcionar continuamente, con procesos automáticos que garantizan su rendimiento, integridad y disponibilidad sin necesidad de intervención directa por parte del usuario final.

6.9 ALTA DISPONIBILIDAD

39. El servicio de Devo está diseñado para ofrecer alta disponibilidad mediante la implementación de arquitecturas cloud redundantes, asegurando que los usuarios puedan acceder a los servicios de manera continua, sin interrupciones. La gestión de la alta disponibilidad es una responsabilidad directa de Devo, que garantiza la operatividad de los servicios a través de diversas estrategias.
40. La combinación de redundancia geográfica, balanceo de carga y capacidades avanzadas de recuperación ante desastres asegura que los usuarios puedan confiar en que los servicios estarán disponibles en todo momento.
41. En caso de que se produzca una interrupción, Devo gestiona el proceso de recuperación, asegurando que el servicio vuelva a estar operativo lo más rápido posible sin intervención del usuario final.

6.10 AUDITORÍA

6.10.1 CAPTURA DE REGISTROS

42. Los cambios generados en el servicio Devo, tales como el *log* in y *log out* de usuarios administradores, son accesibles a través del componente Web Portal, en la sección "*Data search*". Esta auditoría comprende un registro de eventos basado en estas categorías:

    - Log in y log out de usuarios administradores.
    - Cambios en la configuración.
    - Reinicio de contraseñas.
    - Gestión de claves de API, certificados X.509 y tokens.
    - Mecanismos de identificación y autenticación.
    - Acceso y peticiones a los datos.
    - Alertas basadas en los datos.
    - Envío de datos a otro almacenamiento.
    - Búsqueda de datos.

43. Los eventos son almacenados en el siguiente formato "*dd-mm-yyyy hh:mm:ss*", correspondientes a *día*, *mes*, *año*, *hora*, *minuto* y *segundo*, respectivamente.

6.10.2 ALMACENAMIENTO LOCAL

44. Para comprobar los logs locales generados por el componente Devo Relay, se deben seguir los pasos de líneas de comandos referentes a [LOGS-DEVO-RELAY].

6.10.3 ALMACENAMIENTO REMOTO

45. Los registros de auditoría, además de almacenarse localmente como en el caso de los relacionados al componente Devo Relay, se almacenan en AWS EBS (sistema de almacenamiento de AWS EC2). Los registros de auditoría almacenados solo son accesibles por el personal de Devo, mientras que los usuarios finales solamente pueden visualizar sus propios registros en su dominio del portal web de Devo.
46. La transmisión de estos logs se realiza a través de un canal cifrado y seguro haciendo uso de TLSv1.2 o superior.

7 REFERENCIAS

[PORTAL-CONTACTO]	https://www.devo.com/contact/
[NAVEGADORES-COMPATIBLES]	https://docs.devo.com/space/latest/94762521/Getting+started#Supported-browsers
[REGISTRO]	https://docs.devo.com/space/latest/94762547/Sign+up+and+log+in
[WEB]	https://docs.devo.com/space/latest/94762521/Getting+started
[REQUISITOS-UBUNTU]	https://docs.devo.com/space/latest/96469035/Planning+Devo+Relay+deployment
[OPENID]	https://docs.devo.com/space/latest/94763025/OpenID#Setting-up-OpenID-user-authentication
[INSTALACIÓN-DEVO-RELAY]	https://docs.devo.com/space/latest/96469100/Install+Devo+Relay+on+an+Ubuntu+box#Installing-Devo-Relay
[CONFIGURACIÓN-DEVO-RELAY]	https://docs.devo.com/space/latest/96469224/Configuring+Devo+Relay
[CREACIÓN-DOMINIO]	https://docs.devo.com/space/latest/94762547/Sign+up+and+log+in#Create-a-Devo-domain
[CONEXIÓN-DEVO-RELAY]	https://docs.devo.com/space/latest/96469732/Set+up+your+relay
[CONFIGURACIÓN-ELB]	https://docs.devo.com/space/latest/94653692/Event+load+balancers
[ALERTAS]	https://docs.devo.com/space/latest/529170511/Working+with+alert+definitions
[USUARIOS]	https://docs.devo.com/space/latest/94763337/Users+and+roles
[ROLES]	https://docs.devo.com/space/latest/94763681/Role+permissions
[STUNNEL]	https://docs.devo.com/space/latest/96469881/Sending+SSL%2FTLS+encrypted+events+to+the+relay#Install-and-configure-stunnel
[LOGS-DEVO-RELAY]	https://docs.devo.com/space/latest/96469918/Managing+Devo+Relay+using+the+command+line#Check-the-relay-logs

8 ABREVIATURAS

API	Application Programming Interface
AWS	Amazon Web Services
CCN	Centro Criptológico Nacional
CPU	Central Processing Unit
EBS	Elastic Block Store
EC2	Elastic Compute Cloud
ELB	Elastic Load Balancer
ENS	Esquema Nacional de Seguridad
GUI	Graphic User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over TLS
LAN	Local Area Network
NTP	Network Time Protocol
OpenID	OpenID Connect
OS	Operating System
SaaS	Software as a Service
SIEM	Security Information and Event Management
SSL	Secure Sockets Layer
STIC	Seguridad de las Tecnologías de la Información y la Comunicación
SYSLOG	System Logging Protocol
TLS	Transport Layer Security
X.509	Standard defining the format of public key certificates