centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1523

Procedimiento de Empleo Seguro Cryhod de PRIM'x personalizado por EPICOM (.DEF y .GOB)

Junio de 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.11 13:31:52 +02'00'

Centro Criptológico Nacional, 2026

ÍNDICE

1 INTRODUCCIÓN

1. CRYHOD.DEF y CRYHOD.GOB son herramientas de software de cifrado de PRIM'X Technologies personalizadas por EPICOM, que permiten proteger la confidencialidad de los datos almacenados en un disco, cifrando el disco completo o algunas de sus particiones. Este producto protege al usuario del robo de su disco duro, siendo una herramienta adecuada para la protección de datos en ordenadores portátiles. El usuario se debe autenticar al arrancar el ordenador para arrancar el sistema y acceder a los datos. Una vez desbloqueada la partición, el cifrado de los datos es transparente al usuario.
2. CRYHOD.DEF y CRYHOD.GOB pueden utilizarse también para incrementar el nivel de seguridad de las estaciones de trabajo ante la filtración de datos. CRYHOD.DEF y CRYHOD.GOB se pueden desplegar fácilmente en una red de ordenadores que utilicen Directorio Activo, y la configuración se puede realizar utilizando el mecanismo GPO.
3. CRYHOD.DEF y CRYHOD.GOB se ejecutan sobre un sistema operativo Microsoft Windows en sus versiones de 10 a 11, y permite añadir un paso de autenticación adicional en el Pre-boot (antes del arranque) del equipo.
4. Si bien CRYHOD.DEF y CRYHOD.GOB permiten la utilización de varios mecanismos de autenticación, **sólo se autoriza el empleo de mecanismos de autenticación fuerte** (*SmartCard* cualificada en el CPSTIC).

2 OBJETO Y ALCANCE

5. En este documento se indican los requisitos necesarios para el despliegue seguro y la utilización del CRYHOD.DEF y CRYHOD.GOB y su material asociado, de forma que el producto se utilice en las condiciones apropiadas acorde a su certificación y calificación, cuando este producto se utiliza para proteger la información en sistemas bajo el alcance del ENS.
6. Este documento se aplica a los Sistemas de Información (SI) en los que se va a instalar CRYHOD.DEF o CRYHOD.GOB, y está dirigido a:
   a) A los integrantes del departamento de SI que necesiten aplicar las recomendaciones incluidas en este documento;
   b) A los integrantes del departamento de SI que se encarguen del despliegue y/o administración del producto y/o del soporte a los usuarios;
   c) Al Director de Seguridad de la Información (CISO), al que le corresponde determinar la elección de las medidas de seguridad, los métodos de implementación de las mismas y la gestión de la PKI (Infraestructura de clave pública).
7. Algunas recomendaciones también se pueden transmitir a los usuarios finales. Sin embargo, debido a la gran diversidad de escenarios de despliegue la elección de las recomendaciones a aplicar depende del escenario utilizado.
8. En este documento se incluyen recomendaciones relacionadas con el trato con usuarios y administradores, la protección del entorno de ejecución del software, la gestión de las claves de cifrado, y la configuración del producto.
9. El presente documento es aplicable a la versión cualificada de CRYHOD.DEF y CRYHOD.GOB (consultar versión cualificada en el CPSTIC) y aplica a todos los usuarios del producto, debiendo tenerse en cuenta por todas las organizaciones que vayan a utilizar este producto.

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.

d) Apartado 7. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de operación del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. Las aplicaciones CRYHOD.DEF y CRYHOD.GOB son un producto software desarrollado por PRIM´X y personalizado por EPICOM que sólo se distribuye a través de EPICOM[1].
11. El usuario final debe adquirir el producto a través de EPICOM.
12. EPICOM debe proporcionarle al usuario los datos de su cuenta de usuario (usuario/contraseña) y la licencia del producto.
13. El usuario final obtendrá el instalador de la herramienta a través de su único distribuidor, que es EPICOM.
14. El usuario final debe comprobar:
    a) Que la aplicación descargada se corresponde con la que le ha indicado EPICOM. La autenticidad del software descargado se verifica comprobando el hash que EPICOM proporciona para cada versión.
    b) Que la persona que le ha proporcionado la información para obtener el material de instalación de CRYHOD es confiable, es decir, es un representante autorizado de EPICOM.

4.2 ENTORNO DE INSTALACIÓN SEGURO

15. El equipo donde se instale debe estar configurado para arrancar en modo UEFI. Por otra, parte debe de tener habilitada la opción de SECURE BOOT y deshabilitada la opción de FAST BOOT.
16. Se ha de comprobar no se haya instalado ningún otro software de cifrado de disco duro.

4.3 REGISTRO Y LICENCIAS

17. Ver apartado 4.1 ENTREGA SEGURA DEL PRODUCTO del presente documento.

4.4 CONSIDERACIONES PREVIAS

18. Se recomienda hacer una salvaguarda de los datos relevantes del sistema previo a su cifrado. Especialmente si es la primera vez que se configura el producto.
19. Los posibles estados de CRYHOD son:
    a) **APAGADO/CIFRADO:** El equipo está apagado y todo su contenido está cifrado. Cuando el dispositivo se encuentra en este modo:

[1] A partir de este momento referidas como simplemente CRYHOD

i. No es posible acceder a la información contenida en el equipo, aunque sus discos sean extraídos físicamente y conectados a otros equipos.

ii. Todos los parámetros críticos de seguridad (claves y certificados), con los que se cifran los archivos, están protegidos.

b) **PRE-BOOT**: El equipo está encendido, pero no se han introducido las credenciales del acceso mediante la *SmartCard*. Cuando el dispositivo se encuentra en este modo:

i. Es posible acceder a ciertas opciones de mantenimiento del software de cifrado.

ii. No es posible acceder a la información contenida en el equipo, aunque sus discos sean extraídos físicamente y conectados a otros equipos.

iii. Todos los parámetros críticos de seguridad (claves y certificados), con los que se cifran los archivos, están protegidos.

c) AUTENTICADO: El equipo está encendido y la autenticación se ha realizado correctamente. Cuando el dispositivo se encuentra en este modo:

i. Es posible acceder a la información contenida en el equipo. CRYHOD cifra y descifra al vuelo los datos almacenados en el disco cuando el usuario accede a los mismos.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

20. Los componentes básicos del *software* CRYHOD son:

a) Una aplicación *software* que, una vez instalada en el equipo, cifrará automáticamente toda la información que se almacene en su disco.

b) Una tarjeta *SmartCard* cualificada que será utilizada para realizar la autenticación *Pre-boot* para poder acceder al equipo.

5 FASE DE INSTALACIÓN

21. El software CRYHOD debe instalarse en un ordenador que cumpla como mínimo los siguientes requisitos:
    a) Sistema Operativo Windows 10 o superior
    b) Sistema de arranque UEFI compatible con Secure Boot y Device Guard
    c) Procesador de 64-bit con soporte para instrucciones de aceleración criptográfica AES-NI
    d) Almacenamiento libre de 2GiB
22. Para instalar la aplicación CRYHOD en un ordenador con Windows, es necesario utilizar el *instalador* proporcionado por EPICOM.
23. Antes de realizar la instalación, es necesario comprobar la autenticidad del software descargado. Para realizar esta comprobación es necesario utilizar el hash que EPICOM proporciona para cada versión.
24. Para realizar la instalación:
    a) Seleccionar el fichero ejecutable recibido (Instalador "Setup Cryhod.def.es" o "Setup Cryhod.gob.es") en el ordenador en el que se va a realizar la instalación.

    ***NOTA**: Se necesitan permisos de administrador para instalar el producto.*

    b) Ejecutar el fichero de instalación y realizar los pasos indicados por el instalador, seleccionando:
        i. Introducir la clave asociada a la licencia del producto, proporcionada al adquirir el producto.
        ii. En la pantalla de personalización de la instalación seleccionar "Deployment Tools", haciendo clic en el nombre y seleccionando "This feature, and all subfeatures, will be installed on local hard drive".
    c) Una vez instalada la aplicación, es necesario reiniciar el ordenador.
    d) Después del reinicio del PC (tras la instalación), es necesario comprobar que CRYHOD se ha instalado correctamente. Debe aparecer el centro de cifrado de CRYHOD en la barra de notificación del equipo.
25. Para más detalles ver REF6.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

26. Una vez instalado correctamente el software CRYHOD en el ordenador, se deben aplicar una serie de requisitos de la configuración segura, para cumplir con la cualificación de CRYHOD.DEF o CRYHOD.GOB.
27. CRYHOD no es compatible con otros productos de cifrado (exceptuando ZONECENTRAL). Concretamente, se debe comprobar que BitLocker está deshabilitado antes de realizar el cifrado de datos con CRYHOD.
28. Por motivos de seguridad, la instalación de CRYHOD desactiva el modo standby para evitar problemas de uso a los usuarios (que podrían pensar que su ordenador está apagado). Es posible reactivar el modo standby a través de la política P801.
29. El software de cifrado CRYHOD dispone de múltiples opciones de configuración que permiten activar o ajustar las funcionalidades del Sistema en función de las necesidades del usuario y sus requisitos de funcionamiento y seguridad.
30. Para la configuración de las políticas de seguridad se deben seguir las instrucciones incluidas el manual de configuración de la *herramienta "CRYHOD Q.2023 Installation Guide - Reference: PX2221560r1"* REF2.
31. A continuación, se detallan aquellas opciones/políticas de seguridad que deben configurarse obligatoriamente para la utilización de CRYHOD:

ID	Policy Value
P2	*<number>2</number> <label>Disable Private Policies</label> <bool>True</bool>*
P102	*<number>102</number> <label>Disallow password accesses</label> <bool>True</bool>*
P103	*<number>103</number> <label> Disallow key file accesses</label> <bool>True</bool>*
P104	*<number>104</number> <label> Disallow cryptographic tokens accesses</label> <bool>False</bool>*
P105	*<number>105</number> <label>Disable CSP accesses</label> <bool>True</bool>*

ID	Policy Value
P140	*<number>140</number> <label>Relax certificate chain CRL control</label> <bool>False</bool>*
P141	*<number>141</number> <label>Certificates restricted to roots</label> <list> <name>Example CA</name> <val>sha256=XXXXXXXX</val> </list> <list>*
P142	*<number>142</number> <label>Allow out-of-date certificates</label> <bool>False</bool>*
P144	*<number>144</number> <label>Force CRL refresh (hours)</label> <int>1</int>*
P146	*<number>146</number> <label>Relax key usage control for certificates</label> <bool>False</bool>*
P261	*<number>261</number> <label>Code attempts</label> <int>3</int>*
P264	*<number>264</number> <label>Emergency access mode (SOS/TP)</label> <int>1</int>*
P292	*<number>292</number> <label>Hash algorithm</label> <int>4</int>*
P383	*<number>383</number> <label>RSA encryption mode</label> <int>3</int>*
P801	*<number>801</number> <label> Enable standby mode </label> <bool>False</bool>*
P802	*<number>802</number> <label>Do not chain preboot credentials</label> <bool>True</bool>*
P803	*<number>803</number> <label>Preboot credentials chaining to ZoneCentral</label> <int>2</int>*

ID	Policy Value
P804	*<number>804</number> <label>Preboot credential chaining period</label> <int>1</int>*
P805	*<number>805</number> <label>Delete after first chaining</label> <bool>False</bool>*
P822	*<label>Mandatory accesses options</label> <int>1</int>*
P825	*<number>825</number> <label>Enforce users rules</label> <int>0</int>*
P820	*<number>820</number> <label>Encryption directives</label> <list> <name>mount="C:"</name> <val>num=20;crypt=1;user=0;auto=1;mode=full</val> </list> <list> <name>mount="D:"</name> <val>num=30;crypt=1;user=0;auto=1;mode=full</val> </list>*

NOTA: *Completar con las unidades disponibles en el equipo.*

32. Excepcionalmente, cuando CRYHOD se configure **en sistemas aislados** que no dispongan de un sistema de gestión de credenciales de CRYHOD centralizado *on-line* u *off-line* se permitirá la utilización de un usuario de recuperación cuyo acceso se realice mediante contraseña (P102). Esta contraseña debe ser modificada regularme (al menos cada 3 meses) o en caso de que haya sido comprometida. Los criterios de contraseña mínimos serán (P712 a P720):

    a) 12 caracteres de longitud.

    b) 2 mayúsculas.

    c) 2 minúsculas.

    d) 1 carácter especial.

    e) 1 número.

6.2 AUTENTICACIÓN

33. Se definen los siguientes perfiles de operación y administración, todos ellos locales, en el dispositivo:

a) **Usuario:** Se habilita después de superar la autenticación del usuario estándar con éxito. Permite acceder a la información contenida en el disco, pero no tiene privilegios para descifrar el disco de forma permanente.

b) **Administrador:** Se habilita después de superar la autenticación del administrador con éxito. Permite acceder a la información contenida en el disco y tiene privilegios para descifrar el disco de forma permanente. Adicionalmente también puede administrar las opciones de configuración que estén permitidas en las políticas configuradas en el equipo.

c) **Recovery:** Se permite la utilización de usuarios de recuperación para poder realizar tareas de mantenimiento/recuperación del equipo en caso de fallo en el acceso con los usuarios estándar.

34. Adicionalmente se define el perfil de **administrador del equipo**:

    a) Este usuario administrador puede ser local o estar gestionado mediante un gestor centralizado de usuarios tipo LDAP como, por ejemplo, un *Active Directory* de Microsoft.

    b) El usuario administrador del equipo tendrá la capacidad de modificar las políticas del sistema, lo que determinará el funcionamiento del *software*.

35. La tarjeta SmartCard utilizada para autenticarse en el equipo cifrado deberá cumplir las siguientes características:

    a) Estar cualificada para su utilización en sistemas del ENS nivel alto.

    b) Estar certificada, al menos, CC EAL4+ aumentado con ALC_DVS.2, ATE_DPT.2 y AVA_VAN.5.

    c) Algoritmos de hash SHA256 o SHA512.

    d) Algoritmos de firma electrónica RSA, PKCS#1, RSASSA, PSS y ECDSA.

    e) Algoritmos de cifrado simétricos AES-192 y CMAC AES-192.

    f) Algoritmos de cifrado asimétricos RSA, clave entre 3072 y 3840 bits.

    g) Algoritmos de cifrado asimétricos ECC NIST P256, P384 y P521.

    h) Algoritmos cifrado asimétricos ECC Brainpool 256r1, 384r1 y 512r1.

NOTA: *La tarjeta criptográfica de la FNMT cumple con los requisitos exigidos en el párrafo anterior.*

36. Los certificados digitales almacenados en la SmartCard deben tener las siguientes características:

    a) Algoritmo de hash SHA256 o SHA512.

    b) Algoritmo de cifrado asimétrico RSA con longitud de clave entre 3072 y 4096 bits.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

37. CRYHOD puede gestionarse tanto en modo local, mediante las políticas de equipo de Windows (gpedit.msc), como en modo centralizado, utilizando las políticas de seguridad de grupo del Directorio Activo.
38. Las operaciones de administración en el sistema quedan limitadas al usuario administrador del equipo y se requerirá autenticación para la realización de las mismas.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

39. Ver apartado 6.2 AUTENTICACIÓN del presente documento.

6.4 GESTIÓN DE CERTIFICADOS

40. Ver apartado 6.2 AUTENTICACIÓNdel presente documento.

6.5 ACTUALIZACIONES

41. CRYHOD es una aplicación software, y se necesita un instalador de la nueva versión de la aplicación para realizar su actualización.
42. CRYHOD permite la actualización de software sin necesidad de reinstalación siempre que se mantenga el tipo de versión, ya sea .DEF o .GOB.
43. El perfil Administrador puede actualizar el *software* del sistema si se proporcionan los ficheros de actualización adecuados.
44. El usuario final debe acceder a esta actualización a través EPICOM.
45. Antes de realizar la instalación, es necesario que el usuario final compruebe la autenticidad del software descargado, utilizando el hash que EPICOM proporciona para cada versión.
46. Las actualizaciones pueden afectar a la compatibilidad con versiones anteriores, por lo que en caso de duda se deberá consultar a EPICOM.
47. **Siempre debe realizarse una copia de seguridad de la información contenida en el equipo antes de proceder a una actualización.**
48. El usuario debe instalar la nueva versión, ejecutando el fichero de actualización descargado.
49. La instalación de CRYHOD detecta versiones anteriores instaladas. La actualización consiste en la desinstalación y reinstalación del software, sin perder las políticas instaladas y las preferencias del usuario.
50. Una vez ejecutado el fichero de actualización descargado, el software CRYHOD se actualiza a la versión descargada.

51. Después de realizar el proceso de instalación de la nueva versión, es necesario reiniciar el ordenador en el que se ha instalado CRYHOD.
52. Después de realizar la instalación y de reiniciar el ordenador, es necesario comprobar que CRYHOD se ha instalado correctamente.

6.6 AUDITORÍA

6.6.1 REGISTRO DE EVENTOS

53. Ver apartado relacionado con los logs en el documento REF3.

6.7 BACKUP

54. Ver apartado relacionado con los backups en el documento REF3.

7 FASE DE OPERACIÓN

55. El equipo debe permanecer apagado cuando no esté en uso, es decir, CRYHOD debe permanecer en estado AUTENTICADO solo cuando se está operando con él.

7.1 ACCIONES TRAS UN COMPROMISO DE SEGURIDAD

56. Se considera un compromiso de seguridad la pérdida o sustracción de un equipo cuando se encuentra en estado AUTENTICADO, aunque el equipo este hibernado, suspendido o bloqueado.
57. Adicionalmente a las acciones establecidas en la normativa vigente y documentación de procedimientos de emergencia del sistema. Cualquier compromiso deberá ser comunicado inmediatamente al Centro Criptológico Nacional, Departamento PYTEC (C/ Argentona 30, 28023 Madrid, soporte.ccn@cni.es) indicando en el asunto el termino Cryhod y su versión entre corchetes como se muestra a continuación [CRYHOD_DEF] o [CRYHOD_GOB].
58. Como norma general, si un equipo en estado AUTENTICADO se pierde, el usuario lo debe notificar lo antes posible a su AOSTIC y a la Autoridad Criptográfica Nacional (CCN) y enviar un informe del incidente por medios seguros.
59. Como norma general, si un equipo en estado APAGADO o PRE-BOOT se pierde, el usuario lo debe notificar lo antes posible a su AOSTIC.
60. En todo caso, la Autoridad Operacional del sistema deberá estar debidamente informada, y se llevará a cabo una investigación del incidente y una evaluación de daños.

8 REFERENCIAS

61. A continuación, se indica la documentación del fabricante para el manejo del CRYHOD, y los documentos a los que se hace referencia en este documento (disponibles en https://client.primx.fr/Documentation/Product?product=CY):

REF1	PRIM'X CRYHOD Q.2023 Security Target - Reference: PX2221576r5
REF2	CRYHOD Q.2023 Installation Guide - Reference: PX2221560r1
REF3	CRYHOD Q.2023 User Guide - Reference: PX2221558r3
REF4	CRYHOD Q.2023 Quick starting guide - Reference: PX2221559r3
REF5	Signing policies - Implementation Guide - Reference: PX141438r3
REF6	Manual de instalación – Código de documento: EP273E890ZZ02

9 ABREVIATURAS

AES Advanced Encryption Standard

AD Active Directory (Directorio Activo)

BIOS Basic Input/Output System

CCN Centro Criptológico Nacional

CISO Chief Information Security Officer (Director de seguridad de la información)

CPSTIC Catálogo de Productos de Seguridad TIC (Catalogue of TIC security products)

CPU Central Processing Unit

DMA Direct Memory Access

ECC *Elliptic Curves Cryptography*

EFI Extensible Firmware Interface

ENS Esquema Nacional de Seguridad

GPO Group Policy Object

NIST *National Institute of Standards and Technology*

NTFS New Technology File System

OTA One Time Access

PKI Public Key Infraestructure (Infraestructura de clave pública)

SHA Secure Hash Algorithm

SI Sistema de Información

SS0 Single Sign On

SW Software

TIC Tecnologías de la Información y las Comunicaciones