

Guía de Seguridad de las TIC

CCN-STIC 1505

Procedimiento de Empleo Seguro CRYHOD de PRIMX



Diciembre de 2024



Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2024

NIPO: 083-24-300-6

Fecha de Edición: diciembre de 2024

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

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

ÍNDICE

1 INTRODUCCIÓN	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	6
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN.....	7
5 FASE DE INSTALACIÓN.....	8
6 FASE DE CONFIGURACIÓN	9
6.1 MODO DE OPERACIÓN SEGURO	9
6.2 AUTENTICACIÓN.....	11
6.3 ADMINISTRACIÓN DEL PRODUCTO	13
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA	13
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES	13
6.4 GESTIÓN DE CERTIFICADOS.....	13
6.5 ACTUALIZACIONES	13
6.6 AUDITORÍA	14
6.6.1 REGISTRO DE EVENTOS	14
6.7 BACKUP	14
7 FASE DE OPERACIÓN	15
7.1 ACCIONES TRAS UN COMPROMISO DE SEGURIDAD	15
8 REFERENCIAS	16
9 ABREVIATURAS	17

1 INTRODUCCIÓN

1. CRYHOD es una herramienta software de cifrado de PRIM'X Technologies, que permite 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 puede utilizarse también para incrementar el nivel de seguridad de las estaciones de trabajo ante la filtración de datos. CRYHOD se puede desplegar fácilmente en una red de ordenadores que utilicen Directorio Activo, y la configuración se puede realizar utilizando el mecanismo GPO.
3. CRYHOD se ejecuta 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 permite 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 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, 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 (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.
10. En España este producto está cualificado para ENS nivel alto en la familia “Almacenamiento cifrado de datos”.

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

11. La aplicación CRYHOD es un producto software desarrollado por PRIM'X que sólo está disponible para su descarga en la web de PRIM'X (client.primx.eu) o a través de distribuidores autorizados.
12. El usuario final debe adquirir el producto a través de PRIM'X o de un distribuidor oficial.
13. Si el usuario final adquirió el producto a través de PRIM'X, éste debe proporcionarle los datos de su cuenta de usuario (usuario/contraseña) y la licencia del producto.
14. Si el usuario final adquirió el producto a través de un distribuidor oficial, éste debe proporcionarle los datos de su cuenta de usuario (usuario/contraseña) y la licencia del producto.
15. El usuario final obtendrá el instalador de la herramienta desde la web de PRIM'X, accediendo a su cuenta de usuario con el usuario y contraseña que le proporcionaron al adquirir el producto.
16. El usuario final debe comprobar:
 - a) Que la aplicación descargada se corresponde con la que le ha indicado PRIM'X o el distribuidor oficial. La autenticidad del software descargado se verifica comprobando el hash que PRIM'X publica de cada versión en su web.
 - b) Que la persona que le ha proporcionado la información para obtener el material de instalación del CRYHOD es confiable, es decir, es un representante autorizado de PRIM'X o de un distribuidor autorizado. Se verifica comprobando que sea el mismo distribuidor que las licencias del software.

4.2 ENTORNO DE INSTALACIÓN SEGURO

17. El equipo donde se instale debe tener habilitado la opción de BIOS Secure Boot y deshabilitada la opción de FAST BOOT.
18. Se ha de comprobar no se hay instalado ningún otro software de cifrado de disco duro.

4.3 REGISTRO Y LICENCIAS

19. Ver apartado 4.1 del presente documento.

4.4 CONSIDERACIONES PREVIAS

20. 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.

21. 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:
 - 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

22. Los componentes básicos del *software* CRYHOD de PRIM'X 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

23. El software CRYHOD debe instalarse en un ordenador que cumpla como mínimo los siguientes requisitos:
 - a) Windows 10 o superior (compatible con Secure Boot y Device Guard)
 - b) Sistemas de 64-bit
24. Para instalar la aplicación CRYHOD en un ordenador con Windows, es necesario utilizar el *instalador* descargado de la web de PRIM'X (client.primx.eu).
25. Antes de realizar la instalación, es necesario comprobar la autenticidad del software descargado. Para realizar esta comprobación es necesario utilizar el hash de cada versión que PRIM'X publica en su página web (client.primx.eu).
26. Para realizar la instalación:
 - a) Seleccionar el fichero ejecutable descargado (Instalador "Setup Cryhod") 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.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

27. 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.
28. 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.
29. 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.
30. El software de cifrado CRYHOD DE PRIM'X 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.
31. Para la configuración de las políticas de seguridad se deben seguir las instrucciones incluidas el manual de configuración de la *herramienta "CRYHOD Q.2021 Installation Guide - Reference: PX20A1410 v1r1 [REF2]"*.
32. A continuación, se detallan aquellas opciones/políticas de seguridad que deben configurarse obligatoriamente para la utilización de CRYHOD:

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

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

ID	Policy Value
P804	<pre><number>804</number> <label>Preboot credential chaining period</label> <int>1</int></pre>
P805	<pre><number>805</number> <label>Delete after first chaining</label> <bool>False</bool></pre>
P822	<pre><label>Mandatory accesses options</label> <int>1</int></pre>
P825	<pre><number>825</number> <label>Enforce users rules</label> <int>0</int></pre>
P820	<pre><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.</pre>

33. 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 regularmente (al menos cada 3 meses) o en caso de que haya sido comprometida. Los criterios de contraseña mínimos serán (P712 a P720):

- a) 10 caracteres de longitud
- b) 2 mayúsculas.
- c) 2 minúsculas.
- d) 1 carácter especial.
- e) 1 número.

6.2 AUTENTICACIÓN

34. 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.
35. 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*.
36. 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 de cifrado asimétricos ECC Brainpool 256r1, 384r1 y 512r1.

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

37. 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

- 38. 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.
- 39. 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

- 40. Ver apartado 6.2 del presente documento.

6.4 GESTIÓN DE CERTIFICADOS

- 41. Ver apartado 6.2 del presente documento.

6.5 ACTUALIZACIONES

- 42. CRYHOD es una aplicación software, y se necesita un instalador de la nueva versión de la aplicación para realizar su actualización.
- 43. CRYHOD permite la actualización de software sin necesidad de reinstalación.
- 44. El perfil Administrador puede actualizar el *software* del sistema si se proporcionan los ficheros de actualización adecuados.
- 45. El usuario final debe acceder a esta actualización a través de la cuenta de usuario proporcionada por PRIM'X o por el distribuidor autorizado que le proporcionó el producto al adquirirlo.
- 46. El usuario final debe acceder a la página web de PRIM'X (client.primx.eu) y acceder a su cuenta de usuario utilizando las credenciales proporcionadas por PRIM'X o por un distribuidor oficial (ver punto 4.1). Una vez autenticado, el usuario debe descargar el fichero de actualización que contiene la nueva versión de software.
- 47. Antes de realizar la instalación, es necesario que el usuario final compruebe la autenticidad del software descargado, utilizando el hash que PRIM'X publica en su web para cada versión.

48. Las actualizaciones pueden afectar a la compatibilidad con versiones anteriores, por lo que en caso de duda se deberá consultar al distribuidor nacional de CRYHOD.
49. **Siempre debe realizarse una copia de seguridad de la información contenida en el equipo antes de proceder a una actualización.**
50. El usuario debe instalar la nueva versión, ejecutando el fichero de actualización descargado.
51. 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.
52. Una vez ejecutado el fichero de actualización descargado, el software CRYHOD se actualiza a la versión descargada.
53. Después de realizar el proceso de instalación de la nueva versión, es necesario reiniciar el ordenador en el que se ha instalado CRYHOD.
54. 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

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

6.7 BACKUP

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

7 FASE DE OPERACIÓN

57. 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

58. 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.
59. 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 entre corchetes como se muestra a continuación [CRYHOD].
60. 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.
61. 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.
62. 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

63. 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/Certificate> y <https://client.primx.fr/Documentation/Product?product=CY>) :

REF1	PRIM'X CRYHOD Q.2021 Security Target - Reference: PX2091368 v1r6
REF2	CRYHOD Q.2021 Installation Guide - Reference: PX20A1410 v1r1
REF3	CRYHOD Q.2021 User Guide - Reference: PX20A1408r v1r3
REF4	CRYHOD Q.2021 Quick starting guide - Reference: PX20A1409 v1r2
REF5	Signing policies - Implementation Guide - Reference: PX141438 v1r4

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	<i>Elliptic Curves Cryptography</i>
EFI	Extensible Firmware Interface
ENS	Esquema Nacional de Seguridad
GPO	Group Policy Object
NIST	<i>National Institute of Standards and Technology</i>
NTFS	New Technology File System
OTA	One Time Access
PKI	Public Key Infrastructure (Infraestructura de clave pública)
SHA	Secure Hash Algorithm
SI	Sistema de Información
SSO	Single Sign On
SW	Software
TIC	Tecnologías de la Información y las Comunicaciones

