centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1512

Procedimiento de Empleo Seguro
ZONECENTRAL de PRIMX

Diciembre 2024

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-301-1.
Fecha de Edición: diciembre de 2024.

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.12.23 17:30:19 +01'00'

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. **ZONECENTRAL** es una herramienta de cifrado de PRIM'X Technologies, que protege la confidencialidad de los documentos manejados por usuarios autorizados en ordenadores independientes, portátiles o estaciones de trabajo conectados a una red corporativa. El producto realiza el almacenamiento cifrado de archivos, sin modificar sus características, de la manera más transparente posible para los usuarios. Los archivos son cifrados 'en el sitio' (donde quiera que se encuentren) y 'al vuelo' (sin una manipulación especial por parte del usuario). El producto cifra también el fichero de intercambio y elimina los archivos temporales.
2. ZONECENTRAL se puede desplegar fácilmente en una red de ordenadores que utilicen Directorio Activo, y la configuración se puede realizar utilizando el mecanismo GPO.
3. ZONECENTRAL se ejecuta sobre un sistema operativo Microsoft Windows en sus versiones de 10 a 11 o Windows server a partir de la versión de 2019.

2 OBJETO Y ALCANCE

4. En este documento se indican los requisitos necesarios para el despliegue seguro y la utilización de la herramienta ZONECENTRAL, 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.
5. Este documento se aplica a los Sistemas de Información (SI) en los que se va a instalar ZONECENTRAL, 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).
6. 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.
7. 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.
8. El presente documento es aplicable a la versión cualificada de ZONECENTRAL (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.
9. En España este producto está calificado como ENS nivel alto en la familia “Almacenamiento cifrado de datos”.

3 ORGANIZACIÓN DEL DOCUMENTO

10. El documento se organiza en los siguientes apartados:

    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 tareas recomendadas para la fase de operación del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

11. La aplicación ZONECENTRAL es un producto software desarrollado por PRIM´X que sólo está disponible para su descarga en la web de PRIM´X (client.primx.eu).
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 (client.primx.eu), 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 ZONECENTRAL 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 REGISTRO Y LICENCIAS

17. Ver apartado **4.1** del presente documento.

4.3 CONSIDERACIONES PREVIAS

18. Para que el producto opere en un entorno seguro, se deben cumplir los siguientes requisitos:
    a) Los usuarios sólo deben acceder a su información sensible en un entorno confiable (cuando esté solo o con gente que tenga "necesidad de conocer").
    b) El entorno confiable debe permitir a cada usuario introducir sus contraseñas (o números PIN) sin ser observados directamente y sin que otros usuarios o posibles hackers puedan interceptar dichas contraseñas o números PIN (teclados inalámbricos, etc.).

c) Una estructura organizacional adecuada permite a los administradores autenticar al usuario remoto antes de cualquier transmisión de las contraseñas SOS u OTA.

d) Una vez autenticado el usuario, el entorno operacional debe garantizar la confidencialidad de la información sensible y de los datos de autenticación.

e) El hardware debe asegurar una protección efectiva contra escuchas y contra la transmisión de datos no autorizada (firewall configurado adecuadamente, antivirus actualizado, anti-spyware, etc.).

f) Las aplicaciones instaladas en el hardware no deben interferir con el correcto funcionamiento del producto. Además, cualquier operación que el usuario pueda llevar sobre los archivos protegidos por ZONECENTRAL, concretamente a través del uso de aplicaciones, no debe generar copias completas o parciales de estos archivos fuera del del producto, a no ser que se solicite expresamente o cuando es un resultado conocido de la operación solicitada.

g) Los usuarios deben comprobar regularmente el reloj de su estación de trabajo para garantizar la calidad de las funciones relacionadas con la marca de tiempos.

h) En caso de un corte de energía repentino cuando los contenedores están abiertos, el efecto de remanencia de las memorias físicas provoca una persistencia de los datos sensibles en estas memorias que puede durar varias décimas de segundo. Si se produce un evento de este tipo, el usuario no debe dejar desatendido el ordenador durante al menos un minuto (a menos que se restablezca la alimentación antes, en cuyo caso las memorias se reinicializarán cuando el usuario reinicie el sistema).

i) Se deben aplicar las mismas medidas seguridad a las localizaciones de los recursos compartidos en remoto que a las estaciones de trabajo de los usuarios. Del mismo modo, la red que proporciona acceso a estos recursos compartidos debe proporcionar medidas efectivas contra amenazas externas a la organización (dispositivos de partición o filtrado, sondas de detección, etc.). Sólo el administrador tendrá permiso de escritura al recurso compartido al recurso compartido que contiene la lista de accesos.

j) Es imprescindible que los archivos que contienen información sensible se creen y no salgan de las zonas cifradas. El paso a través de zonas no cifradas podría provocar que el sistema operativo realizase alguna manipulación en estos archivos, especialmente en los archivos pequeños (de unos cientos de bytes) que pueden residir durante algún tiempo en el sistema de gestión de archivos NTFS.

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

19. Los componentes básicos del ZONECENTRAL de PRIM'X se reducen a una **aplicación software**.

5 FASE DE INSTALACIÓN

20. El software ZONECENTRAL debe instalarse en un ordenador que cumpla como mínimo los siguientes requisitos:

    a) Sólo puede instalarse en un sistema operativo Windows. Los sistemas operativos compatibles son:

        i. Windows 10 a 11[1]

        ii. Windows Server 2019 (o superior)

21. Para instalar la aplicación ZONECENTRAL en un ordenador con Windows, es necesario utilizar el *instalador* descargado de la web de PRIM'X (client.primx.eu).

22. 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).

23. Para realizar la instalación:

    a) Seleccionar el fichero ejecutable descargado (Instalador "Zone Central Setup") 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 NO seleccionar "ZonePoint" ni "ZedMail for Outlook", haciendo clic en el nombre y seleccionando "This feature will not be available".

    c) Una vez instalada la aplicación, es necesario reiniciar el ordenador.

    d) Después del reinicio del PC (tras la instalación), es necesario comprobar que ZONECENTRAL se ha instalado correctamente. Debe aparecer un menú contextual nuevo cuando se pulse con el botón derecho del ratón sobre el escritorio.

[1] La compatibilidad con Windows 10/11 puede necesitar configuraciones específicas detalladas en https://www.primx.eu/Windows10

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

24. Una vez instalado correctamente el software ZONE CENTRAL en el ordenador, se deben aplicar una serie de requisitos de la configuración segura, para cumplir con la cualificación de ZONE CENTRAL.

25. La configuración de ZONECENTRAL es diferente en función del modo de uso:

    a) Modo Directorio Activo:

        i. La política P131 (mandatory accesses) debe configurarse con acceso de recuperación del administrador.

           Nota: Si se necesita realizar una recuperación de datos, las políticas P269 (Opening zones with recovery keys), P198 (Display recovery accesses) y P199 (Display mandatory accesses) deben estar activadas. Estas políticas normalmente están desabilitadas en un entorno de producción (por ejemplo, para ocultar los accesos de recuperación) y, por tanto, no forman parte del alcance de pruebas de la evaluación.

        ii. La política 278 (alternate temporary folders for the CryptUpdate Agent) debe configurarse con una con una ubicación local de la estación de trabajo (por ejemplo, %USERPROFILE%\EncryptionBackup); y en la política P499 debe configurarse *PreferAlternateBackupLocationsOnNetwork* con el valor «1». También es importante asegurarse de que otros usuarios no tienen acceso de lectura a la ubicación seleccionada.

        iii. La política P702 (maximum password duration) debe configurarse con un valor menor de 90 días.

        iv. La política P710 (Password acceptance threshold) se debe configurar con el valor 100%, y la política P712 (Password length) se debe configurar con el valor 12.

        v. No activar la política P110, para prohibir la autenticación única.

        vi. La política P303 (send event logs for successful management commands) se debe configurar con el valor «yes».

        vii. La política P339 (options of configuration report) debe configurarse con el valor «0» y la política P137 (mandatory accesses for gathered information encryption) debe configurarse con el valor «NONE» en el campo nombre del valor.

        viii. La política P380 (encryption Mechanism) debe configurarse con el valor CTS-3.

        ix. La política P382 (enable use of AES-NI instruction set) debe configurarse con el valor «No» (valor por defecto).

x. La política P383 (RSA Encryption Scheme) debe configurarse con el valor «PKCS#1 v2.2 with SHA-256»

xi. La política P386 (Signature mechanism) debe configurarse con el valor «PKCS#1 v2.2 PSS».

xii. La política P387 (Derivation mechanism (password)) debe configurarse con el valor «SHA256-PBKDF2» o «SHA512-PBKDF2».

xiii. La política P398 (Verification of the integrity of the encrypted zones) debe configurarse con el valor «Verification with warning of absence of integrity data»

b) Modo Alternativo:

i. Todas las políticas indicadas en el apartado anterior (P131, P278, P499, P702, P710, P712, P110, P303, P339, P137, P380, P382, P383, P386, P387 y P398) deben configurarse en el archivo de configuración de políticas del modo alternativo.

ii. Además del archivo de configuración de políticas del modo alternativo, se deben configurar las siguientes políticas en las políticas del directorio activo:

1. La política P070 (alternative policies configuration) se debe configurar con la ruta del archivo de configuración de políticas del modo alternativo.

2. Las GPOs se deben firmar según se indica en la guía proporcionada por PRIM'X.

26. Tanto para el modo Directorio Activo como para el modo Alternativo, las GPOs se deben firmar según se indica en la guía proporcionada por PRIM'X.

27. Además de configurar las políticas indicadas en los párrafos anteriores (que son obligatorias), se recomienda seguir una serie de buenas prácticas, que se describen a continuación:

a) Deshabilitar los tipos de acceso no previstos en los escenarios, utilizando las políticas de la P101 a P105.

b) Autorizar únicamente certificados firmados por las autoridades de certificación de la PKI interna y los de los colaboradores, cumplimentando la política P141.

c) Acceder a las librerías PKCS#11 utilizadas en la política P296 para restringir el uso de tarjetas y tokens a los que están autorizados.

d) Hiberfiles (hiberfil.sys): ZONECENTRAL es compatible con las hibernaciones; las zonas (y las claves de acceso) se cierran automática y correctamente, y los archivos del sistema "caches" se eliminan correctamente. Por lo tanto, las hibernaciones no implican ningún riesgo para ZONECENTRAL. No obstante, ZONECENTRAL no cifra los archivos de hibernación por lo que no los protege (sin embargo, al finalizar la hibernación los detecta y procede

automáticamente a un borrado seguro de su contenido). La información residual en la memoria de la aplicación del usuario en el momento de la hibernación puede permanecer dentro de este archivo (no es el caso de los archivos de intercambio, que sí son cifrados por ZONECENTRAL).

e) Para una seguridad óptima de la estación de trabajo, se recomienda deshabilitar la función de hibernación (y, en su lugar, cerrar la sesión de Windows).

f) "Crash Dumps": ZONECENTRAL no cifra los dumps realizados por Windows en caso de fallo del sistema. Estos dumps pueden contener información residual en la memoria de la aplicación de usuario en el momento del fallo.

g) Para una seguridad óptima del puesto de trabajo, se recomienda deshabilitar la generación de estos dumps.

h) En caso de apagado repentino del ordenador mientras se está cifrando una carpeta, es recomendable notificar al administrador, reiniciar el ordenador y autenticarse con ZONECENTRAL para que el cifrado se reanude automáticamente. Una parada repentina dejará la carpeta en un estado de cifrado incompleto con algunos de los archivos de usuario todavía en claro y algunos archivos técnicos de ZONECENTRAL aún presentes.

i) Enlaces a archivos reales (hardlink): Esta característica permite disponer de varias "vistas" de un mismo archivo, dentro de zonas diferentes (cifradas o sin cifrar).

j) Enlaces a archivos simbólicos: PRIM'X recomienda utilizar estos enlaces con precaución. Si se utilizan, el oficial de seguridad debe asegurarse de que el archivo del enlace y el archivo de destino se encuentren en el mismo estado de cifrado: ambos cifrados (con la misma clave) o ambos sin cifrar.

6.2 AUTENTICACIÓN

28. Se definen tres tipos diferentes de usuario para utilizar ZONECENTRAL (usuarios del producto, operadores del servicio de asistencia y administradores del producto), a los que se les debe aplicar una serie de recomendaciones para cumplir con la cualificación de ZONECENTRAL:

a) El administrador del producto y el operador del servicio de asistencia son personas confiables. Igualmente, los administradores de Windows son personas confiables, responsables de la configuración con valores confiables.

b) La configuración detallada de las políticas, según el alcance de la evaluación, está indicada en la guía de administración del producto (*product administrator guide*) y en el punto 6.1 del presente documento.

c) Cuando por razones prácticas, de logística o de esquemas de organización o de organización, las funciones de administración del equipo se delegan a los usuarios finales, estos usuarios deben recibir formación específicamente

orientada a esas funciones, y las únicas funciones que pueden ser delegadas son las que son absolutamente necesarias.

d) Los usuarios, el operador del servicio de asistencia y el administrador deben recibir formación en el uso del producto y ser conscientes de los problemas de seguridad IT (incluyendo la importancia de la calidad de las claves de acceso y de los dispositivos en los que se almacenan estas claves, cuando se utiliza un soporte físico de administración de clave). El administrador del producto debe recibir formación apropiada para tal fin.

29. A continuación, se indican los requisitos que se deben aplicar a las claves de acceso, para cumplir con la cualificación de ZONECENTRAL:

a) Los administradores del producto deben ser conscientes de la importancia de la calidad de las claves de acceso que proporcionan al producto, para que se cumpla con el estado del arte de su aplicación. Los administradores del producto también deben ser conscientes de la importancia de la calidad del de los dispositivos en los que se almacenan estas claves, cuando se utiliza un soporte físico de administración de clave.

b) El administrador es el responsable de crear las listas de acceso y almacenarlas en un recurso compartido dedicado.

c) El administrador también es responsable, cuando proporciona claves de acceso con un certificado X509, de comprobar la validez de los certificados y su idoneidad para el uso del producto. Este requisito aplica a los certificados raíz “Authenticode”, que se pueden utilizar como base para comprobar la integridad del

d) Los usuarios deben guardar en un lugar seguro las claves que les ha enviado el administrador del producto, además de hacer todo lo posible para evitar su divulgación. El administrador debe guardar sus claves de recuperación y la clave de firma en un lugar Seguro, además de evitar su divulgación.

e) Antes de cualquier cifrado de zona, es imprescindible que el usuario haya hecho un uso considerable del teclado o al menos que haya escrito el equivalente a 3 líneas de texto en lenguaje natural. Estas secuencias tipográficas son en realidad parte de los elementos de ruido que intervienen en el cálculo inicial de los elementos aleatorios utilizados para generar claves de zona.

f) El algoritmo de cifrado RSA se reconoce como estándar si se integra en un módulo mayor o igual de 2048 bits para un uso que no supere los 2030, y si los exponentes públicos son superiores a 65536.

g) A pesar de la recomendación de más abajo, las claves RSA generadas fuera del producto que se incorporan en el archivo de claves o en objetos físicos (para ser utilizadas como claves de acceso) deben ser generadas de acuerdo a las normas y recomendaciones del CCN.

h) El uso de modo SS0 (Single Sign On) hace que el nivel de seguridad proporcionado por el producto sea equivalente al de Windows y, por tanto, no debe utilizarse en condiciones de evaluación (función fuera del ámbito de aplicación).

30. Además de los requisitos indicados en los párrafos anteriores (que son obligatorios), se recomienda seguir una serie de buenas prácticas, que se describen a continuación:

a) Cuando los usuarios dispongan de certificados emitidos por una PKI de confianza, el uso de estos certificados es preferible al uso de contraseñas.

b) Las claves privadas nunca se deben nunca almacenar en claro, y deben estar protegidas por contraseña.

c) El proceso de distribución de la clave a los usuarios finales debe incluir el cambio de la contraseña de protección, una vez se haya recibido la clave.

d) Es preferible el almacenamiento de la clave criptográfica en un soporte criptográfico hardware (smartcard, token PKCS#11, etc.) siempre que sea posible. Se debe utilizar PKCS#11 porque previene contra la extracción de la clave privada.

e) Si se utilizan usuarios PKI, es preferible el uso de técnicas de claves bajo custodia al método de acceso obligatorio a los datos protegidos. Si se define el método de acceso obligatorio, el acceso debe ser particularmente robusto. Se recomienda utilizar un certificado, preferiblemente almacenado en un soporte criptográfico hardware.

f) Se debe renovar la clave de cifrado de la zona cuando se elimina el acceso a la misma.

g) Cuando se llame al servicio de asistencia, es recomendable que el operador verifique la identidad del usuario mediante un procedimiento que ofrezca garantías reales de la identidad de la persona que realiza la llamada. Se recomienda el uso del procedimiento del servicio de asistencia que implique un acceso temporal (configurar la política P264 con el valor “Only One-Time Access”).

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

31. Ver apartados **6.1** y **6.2** del presente documento.

32. ZONECENTRAL 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.

33. 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

34. Ver apartado **6.2** del presente documento.

6.4 GESTIÓN DE CERTIFICADOS

35. Ver apartado **6.2** del presente documento.

6.5 ACTUALIZACIONES

36. ZONECENTRAL es una aplicación software, y se necesita un instalador de la nueva versión de la aplicación para realizar su actualización.
37. 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.
38. 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.
39. 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.
40. Las actualizaciones pueden afectar a la compatibilidad con versiones anteriores, por lo que en caso de duda se deberá consultar al distribuidor nacional de ZONECENTRAL.
41. **Siempre debe realizarse una copia de seguridad de la información contenida en el equipo antes de proceder a una actualización.**
42. El usuario debe instalar la nueva versión, ejecutando el fichero de actualización descargado.
43. La instalación de ZONECENTRAL detecta versiones anteriores instaladas. La actualización consiste en la desinstalación y reinstalación del software, sin perder las políticas instaladas y las preferencias del usuario
44. Una vez ejecutado el fichero de actualización descargado, el software de ZONECENTRAL se actualiza a la versión descargada.
45. Después de realizar el proceso de instalación de la nueva versión, es necesario reiniciar el ordenador en el que se ha instalado ZONECENTRAL.
46. Después de realizar la instalación y de reiniciar el ordenador, es necesario comprobar que la versión de ZONECENTRAL es la correcta.

6.6 AUDITORÍA

6.6.1 REGISTRO DE EVENTOS

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

6.7 BACKUP

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

7 FASE DE OPERACIÓN

7.1 ACCIONES TRAS UN COMPROMISO DE SEGURIDAD

49. 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 ZONECENTRAL entre corchetes como se muestra a continuación [ZONECENTRAL].
50. 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

51. A continuación, se indica la documentación del fabricante para el manejo del ZONECENTRAL, 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=ZC):

REF1	PRIM'X ZONECENTRAL Q.2021 Security Target - Reference: PX20A1373 v1r6
REF2	ZONECENTRAL Q.2021 Installation Guide - Reference: PX20A1392 v1r1
REF3	ZONECENTRAL Q.2021 Encrypted Zones User Guide - Reference: PX20A1387 v1r2
REF4	ZONECENTRAL Q.2021 Administrator Guide - Reference: PX20A1381 v1r3
REF5	Policies Manual Q.2021 - Reference: PX20A1377 v1r2
REF6	ZONECENTRAL 2021 ZoneBoard User Guide - Reference: PX188921 v1r6
REF7	Signing policies - Implementation Guide - Reference: PX141438 v1r5
REF8	ZONECENTRAL Q.2021 Computer pool management using WMI - Reference: PX20A1394 v1r2

9 ABREVIATURAS

AD	Active Directory (Directorio Activo)
AES	Advanced Encryption Standard
CISO	Chief Information Security Officer (Director de seguridad de la información)
CPU	Central Processing Unit
ENS	Esquema Nacional de Seguridad
GPO	Group Policy Object
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

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL