NORMA CUBANA

NC

Obligatoria

EN 1300: 2015
(Publicada por el CEN en 2013)

UNIDADES DE ALMACENAMIENTO SEGURO — CLASIFICACIÓN DE CERRADURAS DE ALTA SEGURIDAD DE ACUERDO CON SU RESISTENCIA A LA APERTURA NO AUTORIZADA (EN 1300: 2013, IDT)

Secure storage units — Classification for high security locks according to their resistance to unauthorized opening

ICS: 13.310

1. Edición Octubre 2015

Oficina Nacional de Normalización (NC) Calle E No. 261 El Vedado, La Habana. Cuba. Teléfono: 78300835 Fax: (537) 836-8048; Correo electrónico: nc@ncnorma.cu; Sitio Web: www.nc.cubaindustria.cu

Cuban National Bureau of Standards

Prefacio

La Oficina Nacional de Normalización (NC), es el Órgano Nacional de Normalización de la República de Cuba y representa al país ante las organizaciones internacionales y regionales de normalización.

La elaboración de las Normas Cubanas y otros documentos normativos relacionados se realiza generalmente a través de los Comités Técnicos de Normalización. Su aprobación es competencia de la Oficina Nacional de Normalización y se basa en las evidencias del consenso.

Esta Norma Cubana:

- Ha sido elaborada por el Comité Técnico de Normalización NC/CTN 51 de Seguridad y protección de las instalaciones, integrado por representantes de las siguientes entidades:

    - Ministerio del Interior (MININT)
    - Oficina del Historiador de La Habana (OHLH)
    - Ministerio de Relaciones Exteriores (MINREX)
    - Ministerio de la Construcción (MICONS)
    - Ministerio de Energía y Minas (MINEM)
    - Instituto Nacional de Recursos Hidráulicos (INRH)
    - Ministerio del Turismo (MINTUR)
    - Ministerio de Salud Pública (MINSAP)
    - Ministerio de Comunicaciones (MICOM)
    - Ministerio del Transporte CACSA (MITRANS)
    - Banco Central de Cuba (BCC)
    - Aduana General de la República. (AGR)

- Es una adopción idéntica por el método de endoso de la versión oficial en español de la Norma Europea EN 1300: 2013 de igual título.

- Incluye los Anexos A, B y C normativos y D y E informativos.

(Página en blanco)

Índice

Unidades de almacenamiento seguro
Clasificación de cerraduras de alta seguridad
de acuerdo con su resistencia a la apertura no autorizada

PRÓLOGO

Esta Norma EN 1300:2013 ha sido elaborada por el Comité Técnico CEN/TC 263 *Almacenamiento seguro de dinero, valores y soportes de datos*, cuya Secretaría desempeña BSI.

Esta norma europea debe recibir el rango de norma nacional mediante la publicación de un texto idéntico a ella o mediante ratificación antes de finales de mayo de 2014, y todas las normas nacionales técnicamente divergentes deben anularse antes de finales de mayo de 2014.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento estén sujetos a derechos de patente. CEN y/o CENELEC no es(son) responsable(s) de la identificación de dichos derechos de patente.

Esta norma anula y sustituye a la Norma EN 1300:2004+A1:2011.

En comparación con la Norma EN 1300:2004+A1:2011, se han realizado las siguientes modificaciones:

- adición de definiciones (capítulo 3) y requisitos (apartado 5.1.6) para los sistemas electrónicos de proximidad;
- adición de definiciones (capítulo 3) y requisitos (apartado 5.1.7) para la criptografía en sistemas de seguridad distribuidos;
- actualización de referencias a las nuevas versiones;
- modificación de los requisitos para la unidad de entrada (apartado 5.1.5.4);
- actualización de las muestras de ensayo de las cerraduras operadas por llave, solicitando que la llave valida sea la de corte de altura media de las tres que se presenten (apartado 7.3);
- aclaración y optimización del ensayo de inmersión (apartado 8.2.6.3);
- corrección del ensayo de resistencia al calor (apartado 8.2.7.2);
- aclaraciones editoriales de varios apartados, entre otros los apartados 5.1.5.1, 5.2.7, 5.3.3, 7.1, 8.2.2.1, 8.2.4.3.2, 8.2.6.2 y 8.3.3.3.2;
- adición de parámetros para las instrucciones de funcionamiento en el anexo A.

Esta norma refleja la demanda del mercado en cuanto a incluir los requisitos para los sistemas distribuidos y los activadores electrónicos, y responde a las exigencias del momento en que fue desarrollada.

Esta norma europea ha sido elaborada por el grupo de trabajo 3 del CEN/TC 263, dentro de la serie de normas dedicadas al almacenamiento seguro de dinero, valores y soportes de datos. Otras normas de esta serie son, entre otras, las siguientes:

- EN 1047-1, *Unidades de almacenamiento de seguridad. Clasificación y métodos de ensayo de resistencia al fuego. Parte 1: Muebles ignífugos y contenedores para soportes sensibles.*
- EN 1047-2, *Unidades de almacenamiento de seguridad. Clasificación y métodos de ensayo de resistencia al fuego. Parte 2: Cámaras y contenedores ignífugos.*
- EN 1143-1, *Unidades de almacenamiento de seguridad. Requisitos, clasificación y métodos de ensayo para resistencia al robo. Parte 1: Cajas fuertes, cajeros automáticos, puertas y cámaras acorazadas.*

- EN 1143-2, *Unidades de almacenamiento de seguridad. Requisitos, clasificación y métodos de ensayo para resistencia al robo. Parte 2: Sistemas de depósito.*

- EN 14450, *Unidades de almacenamiento de seguridad. Requisitos, clasificación y métodos de ensayo para resistencia al robo. Cajas de seguridad.*

De acuerdo con el Reglamento Interior de CEN/CENELEC, están obligados a adoptar esta norma europea los organismos de normalización de los siguientes países: Alemania, Antigua República Yugoslava de Macedonia, Austria, Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Letonia, Lituania, Luxemburgo, Malta, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Rumanía, Suecia, Suiza y Turquía.

0 Introducción

Esta norma europea también especifica los requisitos para las cerraduras electrónicas de alta seguridad – CAS (HSL, *High security electronic locks*) controladas remotamente. En cuanto a los sistemas distribuidos, esta norma responde al diseño requerido en el entorno tecnológico del momento en que se elaboró. Es obligatorio que esta norma se revise cada 3 años, ya que la investigación en el área de la criptografía y los medios de ataque evolucionan muy rápidamente, así como las normas citadas.

1 Objeto y campo de aplicación

Esta norma europea especifica los requisitos para las cerraduras de alta seguridad (CAS/HSL) en cuanto a fiabilidad, resistencia al robo y apertura no autorizada, junto con sus métodos de ensayo. También incluye un esquema para la clasificación de las CAS, de conformidad con el grado otorgado de resistencia al robo y apertura no autorizada.

Esta norma se aplica tanto a las CAS mecánicas como a las electrónicas. Las siguientes prestaciones pueden incluirse de forma opcional, ya que no son obligatorias:

a) código maestro para evitar la alteración del código base y/o la activación/desactivación de códigos paralelos;

b) código maestro para desactivar las funciones de tiempo;

c) integración de componentes o funciones de alarma;

d) funciones del control remoto;

e) resistencia al ataque con ácidos;

f) resistencia a los rayos X;

g) resistencia a los explosivos;

h) funciones de tiempo.

2 Normas para consulta

Los documentos indicados a continuación, en su totalidad o en parte, son normas para consulta indispensables para la aplicación de este documento. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición (incluyendo cualquier modificación de ésta).

EN 1143-1, *Unidades de almacenamiento de seguridad. Requisitos, clasificación y métodos de ensayo para resistencia al robo. Parte 1: Cajas fuertes, cajeros automáticos, puertas y cámaras acorazadas.*

EN 60068-2-1:2007, *Ensayos ambientales. Parte 2-1: Ensayos. Ensayo A: Frío. (IEC 60068-2-1:2007).*

EN 60068-2-2:2007, *Ensayos ambientales. Parte 2-2: Ensayos. Ensayo B: Calor seco. (IEC 60068-2-2:2007).*

EN 60068-2-6:2008, *Ensayos ambientales. Parte 2-6: Ensayos. Ensayo Fc: Vibración (sinusoidal). (IEC 60068-2-6:2007).*

EN 60068-2-17:1994, *Ensayos ambientales. Parte 2: Ensayos. Ensayo Q: Estanquidad. (IEC 60068-2-17:1994).*

EN 61000-4-2, *Compatibilidad electromagnética (CEM). Parte 4: Técnicas de ensayo y de medida. Sección 2: Ensayos de inmunidad a las descargas electrostáticas. Norma básica de CEM. (IEC 61000-4-2).*

EN 61000-4-3, *Compatibilidad electromagnética (CEM). Parte 4-3: Técnicas de ensayo y de medida. Ensayos de inmunidad a los campos electromagnéticos, radiados y de radiofrecuencia. (IEC 61000-4-3).*

EN 61000-4-4, *Compatibilidad electromagnética (CEM). Parte 4-4: Técnicas de ensayo y de medida. Ensayos de inmunidad a los transitorios eléctricos rápidos en ráfagas.(IEC 61000-4-4).*

EN 61000-4-5, *Compatibilidad electromagnética (CEM). Parte 4-5: Técnicas de ensayo y de medida. Ensayos de inmunidad a las ondas de choque. (IEC 61000-4-5).*

EN 61000-4-6, *Compatibilidad electromagnética (CEM). Parte 4-6: Técnicas de ensayo y de medida. Inmunidad a las perturbaciones conducidas, inducidas por los campos de radiofrecuencia. (IEC 61000-4-6).*

EN ISO 6988, *Recubrimientos metálicos y otros recubrimientos no orgánicos. Ensayo al dióxido de azufre con condensación general de la humedad. (ISO 6988).*

ISO/IEC 9798-1:2010, *Tecnología de la información. Técnicas de Seguridad. Autentificación del usuario. Parte 1: Generalidades.*

ISO/IEC 9798-2, *Tecnología de la información. Técnicas de Seguridad. Autentificación del usuario. Parte 2: Mecanismos que utilizan algoritmos para encriptación simétricos.*

ISO/IEC 9798-4, *Tecnología de la información. Técnicas de Seguridad. Autentificación del usuario. Parte 4: Mecanismos que utilizan una función de chequeo criptográfico.*

3 Términos y definiciones

Para los fines de este documento, se aplican los términos y definiciones siguientes:

3.1 cerradura de alta seguridad, CAS:
Elemento independiente, normalmente montado en las puertas de las unidades de almacenamiento de seguridad.

NOTA Los códigos pueden introducirse en una CAS por comparación con los memorizados (unidad de procesamiento). El código de apertura correcto permite el accionamiento del sistema de bloqueo.

3.2 código:
Información de identificación requerida, que puede introducirse en una CAS, y si es correcta, permite modificar el estado de seguridad de la CAS.

3.2.1 código de apertura:
Información de identificación que permite la apertura de la CAS.

3.2.2 código reconocido:
Información de identificación que permite el acceso a la unidad de procesamiento y que también puede ser un código de apertura.

3.2.3 código de coacción:
Código paralelo que inicia determinadas funciones adicionales.

3.2.4 código paralelo:
Código de apertura con idéntica función que la del código de apertura ya existente, pero constituido por información diferente.

3.3 medios de codificación:
Método por el cual se instala el código.

3.3.1 código material:
Código definido por las características físicas u otras propiedades de un soporte físico.

3.3.2 código nemotécnico:
Código memorizable compuesto por información numérica y/o alfabética.

3.3.3 código biométrico:
Código basado en características de la persona.

3.3.4 código de un solo uso:
Código que cambia tras cada uso generado mediante un algoritmo.

3.4 unidad de entrada:
Componente de una CAS que recibe y transmite los códigos a la unidad de procesamiento.

3.5 unidad de procesamiento:
Componente de una CAS que evalúa si el código de entrada es correcto o no, y en base a ello autoriza o deniega el funcionamiento del mecanismo de cierre.

3.6 mecanismo de cierre:
Pestillo o pestillos que forman parte de una CAS, cuya función es permitir o impedir la apertura del sistema de bloqueo.

3.7 autentificador:
Elemento cuyo formato físico o propiedades determinan un código reconocido, por ejemplo una llave.

NOTA Un autentificador electrónico incorpora un circuito integrado que contiene una memoria volátil o no, una aplicación asociada y en muchos casos un micro-controlador, que comunica con la unidad de entrada por medio de contacto o por proximidad.

3.8 CAS mecánica:
CAS asegurada exclusivamente por elementos de seguridad mecánicos.

3.9 CAS electrónica:
CAS asegurada, parcial o totalmente, por elementos de seguridad eléctricos o electrónicos.

3.10 mecanismo de bloqueo:
Componente de una CAS que, tras la introducción del código de apertura correcto, se mueve o permite su movimiento.

NOTA El elemento de bloqueo permite asegurar una puerta o impedir el movimiento de la pestillería. El pestillo de una CAS mecánica es un ejemplo de elemento de bloqueo.

3.11 robo destructivo:
Ataque a la CAS de tal forma que le produce daños irreversibles y que no pueden ser ocultados al usuario autorizado.

3.12 fiabilidad:
Capacidad de funcionar y cumplir con los requisitos de seguridad de esta norma, tras un elevado número de ciclos de utilización.

3.13 manipulación:
Método de ataque cuyo fin es desactivar la función de bloqueo sin causar daños perceptibles para el usuario.

NOTA Una CAS puede funcionar tras una manipulación aunque su seguridad pudiera estar degradada permanentemente.

3.14 espionaje:
Intento de obtener información no autorizada.

3.15 códigos utilizables:
Son los códigos o autentificadores permitidos por el fabricante y que cumplen con los requisitos de esta norma.

NOTA Para las CAS mecánicas el número de códigos utilizables es mucho menor que el número total de códigos para el cual se puede preparar la CAS.

3.16 condición de codificación aleatoria:
Configuración en la que los elementos de codificación tienen la configuración necesaria para no permitir la apertura de la CAS si no se introduce el código correcto completo o el autentificador adecuado.

3.17 secuencia de cerrado:
Serie de acciones que empiezan con la puerta abierta y que terminan cuando su cierre es efectivo: puerta cerrada con sus pestillos extendidos, bloqueada y asegurada.

3.18 puerta abierta:
Puerta que no está alineada con su marco.

3.19 puerta cerrada:
Puerta que está alineada con su marco y preparada para extender su pestillería.

3.20 puerta cerrada con pestillo:
Puerta que está alineada con su marco y pestillos extendidos echados.

3.21 puerta bloqueada:
Puerta cerrada con la pestillería extendida y que no puede abrirse sin la activación de la CAS.

3.22 puerta asegurada:
Puerta cerrada, con los pestillos extendidos y bloqueada con su sistema de bloqueo en situación de CAS asegurada.

3.23 condición de CAS asegurada:
El dispositivo de bloqueo está activado y sólo puede desbloquearse introduciendo el(los) código(s) de apertura.

3.24 condición normal:
Tras el ensayo la muestra está en situación de CAS asegurada y todas sus funciones operativas.

3.25 condición operativa:
Tras el ensayo, la muestra está en situación de CAS asegurada, pudiendo ser desbloqueada con el(los) código(s) de apertura, aunque no todas sus funciones permanezcan operativas.

3.26 fallo de seguridad:
Tras el ensayo, la muestra está en situación de CAS asegurada, pero no tiene operativas todas las funciones de diseño, y por lo tanto no puede ser abierta con el(los) código(s) de apertura.

3.27 unidad de resistencia, RU:
Es el valor de la resistencia al robo y a la manipulación.

NOTA Resultado del cálculo en base al tipo de herramienta utilizada y al daño causado en un tiempo determinado.

3.28 tiempo de penalización:
Periodo de inactividad de CAS impuesto por exceso de intentos de apertura.

3.29 autenticación:
Método para prevención del fraude mediante el aseguramiento de que la comunicación, entre los componentes de un sistema distribuido, solo puede ser establecida tras confirmar la adecuada identificación de los mismos.

3.30 algoritmo criptográfico:
Método matemático para la transformación de los datos que incluye la definición de parámetros (por ejemplo la longitud de la clave y el número de repeticiones o vueltas).

3.30.1 algoritmo criptográfico asimétrico:
Algoritmo criptográfico que utiliza dos claves relacionadas, una pública y una privada, que tienen la propiedad de que el uso independiente de las mismas es informáticamente imposible.

3.30.2 algoritmo criptográfico simétrico:
Algoritmo criptográfico que utiliza una única clave secreta para la encriptación y la desencriptación.

3.31 clave criptográfica:
Parámetro utilizado conjuntamente con un algoritmo criptográfico que se usa para controlar un proceso criptográfico tal como encriptación, desencriptación o autenticación

NOTA El conocimiento de la clave adecuada permite la correcta encriptación y/o desencriptación, o la validación de un mensaje.

3.32 módulo criptográfico:
Conjunto de hardware y software que implementa las funciones de seguridad para los sistemas distribuidos y los autentificadores electrónicos, incluyendo los algoritmos criptográficos.

3.33 sistema distribuido:
Sistema con varios componentes conectados entre sí por un medio de transmisión, tanto si es cableado como si no.

NOTA Se supone que la información transmitida puede ser accesible para una tercera parte. Una CAS con componentes en ubicaciones separadas se define como un sistema distribuido. Un sistema con dos unidades de entrada, una en el contenedor y otra en remoto (= unidad de entrada distribuida) es un ejemplo de un sistema distribuido. Una cerradura electrónica con un sistema de transmisión no accesible, según se determina en el apartado 5.1.5.3 de esta norma, o con una conexión temporal cableada in situ a un equipo móvil (por ejemplo un ordenador personal), supervisado por una persona autorizada, no se considera como un sistema distribuido.

3.34 encriptación:
Es el procedimiento que convierte un mensaje o archivo en ininteligible para cualquiera que no esté autorizado a leerlo.

NOTA Durante el proceso de encriptación, un algoritmo criptográfico que utilice la clave criptográfica se usa para transformar un texto normal en texto cifrado. Este procedimiento consta de:

- un modo operativo, que define la manera en que se procesan los datos con el algoritmo.
- un esquema de cifrado, que define la manera como se componen las cadenas de datos de una longitud determinada.

3.35 sistema de transmisión:
Es el sistema de comunicación entre los componentes de un sistema distribuido.

NOTA Pueden utilizarse como vía de transmisión las líneas dedicadas, las redes públicas conmutadas cableadas o inalámbricas.

3.36 información relevante de seguridad:
Se consideran como tal los códigos (de conformidad con el apartado 3.2), las autenticaciones, cualquier código o clave de transmisión y sus modificaciones, así como las actualizaciones de la programación de las unidades de procesamiento.

3.37 intercambio automático de clave:
Se trata de un protocolo que permite a dos componentes, que podrían no tener conocimiento previo el uno del otro, establecer una clave secreta compartida a través de un canal de comunicación no seguro.

3.38 disponibilidad:
Tiempo durante el cual el sistema se encuentra en condiciones normales de funcionamiento.

4 Clasificación

Las CAS se clasifican en varias clases (A, B, C o D) según se la tabla 1 (Requisitos de seguridad), la tabla 2 (Resistencia electromagnética) y la tabla 3 (Resistencia a la vibración), en base a sus requisitos de seguridad. Se debe cumplir con los requisitos generales de seguridad y fiabilidad (véanse 5.1, 5.2 y 5.3).

NOTA Las CAS de clase A tienen los menores requisitos y las de clase D los más altos.

5 Requisitos

5.1 Requisitos generales

Todos los requisitos deben ensayarse de conformidad con el apartado 8.1.2.

5.1.1 Requisitos para todas las clases

5.1.1.1 Las CAS solamente deben abrirse por los códigos de apertura válidos. Los códigos de apertura deben mantenerse como los únicos códigos válidos de apertura hasta que se modifiquen formalmente. No se permiten los códigos sobrepuestos o indocumentados.

5.1.1.2 Cuando se utilicen códigos nemotécnicos en una CAS, debe ser posible su modificación.

5.1.1.3 Debe ser imposible poder utilizar un dispositivo suplementario (por ejemplo un micro interruptor) instalado por el fabricante en la CAS para obtener información sobre el código.

5.1.1.4 La unidad de entrada es un componente esencial de una CAS, aunque esa unidad pueda operar más de una CAS (unidad procesadora). Cada CAS debe tener una unidad procesadora que acepte el código correcto proporcionado por la unidad de entrada. Cada CAS debe incorporar también, o en su caso ser capaz de activar/desactivar, el mecanismo de bloqueo. Si dicho mecanismo debiese activarse antes del primer uso, se debe incluir una nota en este sentido en las instrucciones de uso de la cerradura.

5.1.1.5 Si el mecanismo de bloqueo no se activa manualmente debe disponer de un medio que indique si la CAS ha sido asegurada, cerrada y bloqueada.

5.1.1.6 Un código de apertura no debe poder modificarse o cambiarse por ningún otro código que no sea un código reconocido.

5.1.2 CAS clase D

5.1.2.1 Deben disponer de un dispositivo que refleje el estado del cierre, bloqueado o desbloqueado.

5.1.2.2 Las CAS con combinación mecánica deben pasar a condición de codificación aleatoria inmediatamente tras el bloqueo.

5.1.2.3 Una CAS de clase D debe incorporar un dispositivo que indique la condición de codificación aleatoria

5.1.3 CAS mecánicas operadas con llave

5.1.3.1 Para las CAS de clase A (véase el capítulo 4) no se debe repetir el mismo código, hasta que por lo menos el 80% de los códigos posibles se hayan utilizado.

5.1.3.2 Los códigos (y los juegos de autentificadores de códigos) deben elegirse al azar.

5.1.3.3 No debe haber números o marcas en los autentificadores o en la CAS que permitan identificar el código. Asimismo no se debe emitir una tarjeta escrita con dicha información.

5.1.3.4 No debe ser posible retirar la llave de la CAS mientras que se encuentre en posición abierta, excepto para el cambio de código. Este requisito es aplicable a todas las clases de CAS. Se admite la posibilidad de activar este mecanismo inmediatamente antes del primer uso de la CAS.

5.1.3.5 La llave no debe romperse bajo la aplicación de un par máximo de 2,5 Nm. Este ensayo debe realizarse según el apartado 8.2.1.4.

5.1.3.6 Además de los requisitos ya mencionados, el fabricante debe cumplimentar también la declaración incluida en el anexo C.

5.1.4 Alturas de las levas para cerraduras mecánicas de llave

5.1.4.1 Los códigos utilizables no deben tener más del 40% de los elementos codificadores (gorjas o levas) de la misma altura.

5.1.4.2 Los códigos utilizables no deben tener más de dos elementos codificadores colindantes iguales (por ejemplo dos levas contiguas con la misma altura).

5.1.4.3 En los códigos utilizables, la diferencia entre la mayor y menor altura de las levas debe ser superior al 60% de la máxima diferencia admisible por la CAS.

5.1.5 CAS Electrónicas

5.1.5.1 Las CAS electrónicas de clase B y con más de 2 códigos de usuarios deben disponer de un registro de las aperturas realizadas, de acuerdo con la tabla 1, y deben tener la posibilidad de guardar esa información durante 1 año por lo menos, incluso en el caso de fallo del suministro eléctrico.

5.1.5.2 Cuando una CAS electrónica esté asegurada, las comunicaciones con la unidad procesadora solo deben ser posibles mediante la introducción de un código reconocido y para mostrar el estado del cierre.

5.1.5.3 Todos los componentes de la unidad de entrada, en los sistemas no distribuidos, deben estar firmemente fijados a la unidad de almacenamiento de seguridad. Con la unidad de entrada fijada a la unidad de almacenamiento de seguridad, el cableado que conecta la unidad de entrada con la unidad procesadora no debe ser accesible.

5.1.5.4 En las CAS de clase C y D, cualquier intento de manipulación o sustitución de la unidad de entrada debe generar una registro en el histórico de eventos y mostrar automáticamente en el display esta información a los sucesivos usuarios, hasta que este aviso sea neutralizado por la persona autorizada.

5.1.5.5 Si el tiempo de penalización estuviese activado debe indicarse claramente a los usuarios, en todas las clases de CAS.

5.1.5.6 Indicador de batería baja: las CAS alimentadas con batería deben ser capaces de realizar como mínimo 3 000 aperturas completas de la cerradura. La capacidad de la batería debe estar monitorizada. En caso de batería(s) baja(s) se debe producir una señal acústica o visible durante o inmediatamente después de un proceso de apertura. Tras el primer aviso de batería baja, todavía deben ser posibles al menos diez (10) procesos completos de apertura y cierre. Cuando sea posible conectar suministro eléctrico externo no será necesario cumplir con este requisito.

5.1.5.7 La unidad de procesamiento para la validación de los códigos debe instalarse en el interior de la unidad de almacenamiento de seguridad.

5.1.5.8 Las CAS electrónicas, a partir de la clase B, deben ensayarse contra las influencias de los campos eléctricos según el apartado 8.2.5.

5.1.6 Autentificadores electrónicos

5.1.6.1 Generalidades

El fabricante debe informar en el manual del equipo que los autentificadores electrónicos deben asegurarse igual que las llaves mecánicas.

5.1.6.2 Autentificadores electrónicos de proximidad

5.1.6.2.1 Generalidades

Los siguientes requisitos, para los autentificadores electrónicos de proximidad, son aplicables solo en las cercanías de equipos de comunicaciones, cuando la distancia normal de funcionamiento sea menor de 15 cm (por ejemplo NFC o Mifare).

Si la separación para la transmisión de datos típica entre el autentificador electrónico y la unidad de lectura fuese superior a 15 cm, o la referida red se utilizase para una CAS de clase D, deben cumplirse los requisitos del apartado 5.1.7 para sistemas distribuidos.

NOTA Los sistemas ópticos se consideran como sistemas distribuidos. Un ejemplo de autentificador activador electrónico de proximidad serían las tarjetas RFID.

5.1.6.2.2 Autenticación mutua

Debe utilizarse la autenticación mutua, de conformidad con la Norma ISO/IEC 9798-2 o la Norma ISO/IEC 9798-4. El parámetro de temporización variable, tipo *time stamp*, secuencia numérica o numeración aleatoria, para impedir una validación auténtica de información posteriormente o más de una vez (véase el anexo B de la Norma ISO/IEC 9798-1:2010), debe contener 32 bits por lo menos. Además, para la autenticación mutua, debe utilizarse un código reconocido que permita la apertura de la CAS.

5.1.6.2.3 Clave criptográfica

La clave criptográfica para algoritmos simétricos debe contener una longitud mínima de 64 bits en las CAS de clase A y B, y de 128 bits para las de clase C y D, y debe programarse exclusivamente para cada modelo específico de CAS. Los algoritmos asimétricos deben tener longitudes de clave similares, en función del nivel de seguridad (NIST SP 800-57). La clave criptográfica para algoritmos simétricos o la clave privada para algoritmos asimétricos, no deben enviarse nunca fuera del autentificador. Puede ser parte de los datos de comunicación transmitidos al autentificador con la finalidad de inicialización. El proceso de inicialización tiene que ser ejecutado por una persona autorizada en un entorno seguro. Esto debe quedar especificado en las instrucciones de uso.

5.1.6.2.4 Número de identificación

Todos los autentificadores electrónicos deben disponer de un número único de identificación. El número de identificación debe disponer de 32 bits de longitud por lo menos. Normalmente, el número de identificación solo se requiere por razones de auditoría. Si el número de serie se utiliza también como información relevante de seguridad, no debe ser visible en el autentificador.

5.1.6.3 Autentificadores electrónicos de contacto

Los autentificadores electrónicos de contacto para las cerraduras diferentes de las de clase D, no tienen que cumplir con los mismos requisitos adicionales de los autentificadores electrónicos de proximidad. En ese caso el fabricante debe especificar en sus manuales si alguna información relevante de seguridad se almacena sin encriptar.

La información relevante de seguridad debería almacenarse de manera segura en el autentificador y debería tener una autentificación segura.

5.1.6.4 Multi-uso (solo válido en CAS de clase B, C y D)

Si el autentificador electrónico se diseña para utilizarse en aplicaciones distintas a la CAS, la información relevante de seguridad no debe ser accesible a dichas otras aplicaciones.

Si el autentificador electrónico no está protegido contra el multi-uso, la siguiente indicación debe incluirse en el manual: *Nunca usar este autentificador electrónico en aplicaciones distintas a las de este modelo de CAS.*

5.1.7 Requisitos criptográficos en los sistemas de seguridad distribuidos

5.1.7.1 Seguridad de la información

5.1.7.1.1 Generalidades

Este apartado se enfoca en la confidencialidad, autenticación, integridad, disponibilidad, transmisión de datos, almacenamiento de información, claves criptográficas y su gestión.

5.1.7.1.2 Confidencialidad

La información relevante de seguridad que se transmite a través de un sistema distribuido, debe encriptarse para impedir lecturas no autorizadas. Para los procesos de transmisión de datos relevantes en sistemas distribuidos, se deben aplicar los requisitos mínimos determinados para los algoritmos simétricos, tales como los bloques TDEA de 64 bits y AES de 128 bits, de conformidad con los documentos NIST SP 800-67 y FIPS 197 respectivamente. Los algoritmos encriptados deben utilizarse en modos seguros de operativa, tales como CBC, CFB y GCM.

5.1.7.1.3 Autenticación

La autenticación se requiere para iniciar la comunicación entre los componentes de un sistema distribuido. El fabricante debe describir el método de autenticación.

5.1.7.1.4 Integridad

Debe verificarse la integridad de los datos para asegurar que no han sido alterados, de forma no autorizada, desde que fueron creados, transmitidos o archivados. Esto incluye la inserción, borrado o sustitución de datos. Los métodos aceptados para asegurar dicha integridad son los algoritmos MAC o las firmas digitales.

5.1.7.1.5 Disponibilidad

Si un sistema distribuido no estuviese disponible temporalmente, dicha situación no debe comprometer el nivel de seguridad.

5.1.7.1.6 Almacenamiento de la información relevante de seguridad

Para el archivo de información de seguridad relevante en las CAS de clase A, se puede optar por utilizar requisitos menores a los indicados en el apartado 5.1.7.1.2 o no encriptación.

5.1.7.1.7 Gestión de una clave criptográfica

Las claves criptográficas deben protegerse contra accesos no autorizados. El fabricante debe definir los métodos de archivo, creación, transmisión acceso a las claves criptográficas. Estos requisitos son también de aplicación al procedimiento de inicialización del fabricante.

5.1.7.1.8 Transmisión de datos para claves criptográficas

Los sistemas distribuidos deben disponer de claves criptográficas generadas aleatoriamente, excepto para la programación inicial de fábrica de las CAS de clases B, C y D. Para la generación de números aleatorios se deben considerar los requisitos del documento FIPS Pub 140-2 4.7.1 (generadores de números aleatorios).

Las claves criptográficas deben poder modificarse in situ en la propia CAS, a partir de la clase B. Asimismo lo pueden ser en las de clase A. Si se codifica una nueva clave esta debe ser la única utilizable.

5.1.7.1.9 Modificación de claves criptográficas

5.1.7.1.9.1 Generalidades

La clave criptográfica inicial de fábrica debe modificarse antes de que el sistema distribuido se active. Si la clave criptográfica no se puede modificar in situ (solo en el caso de CAS de clase A), deben implementarse las precauciones necesarias para impedir que el personal directamente involucrado en la fabricación de la cerradura sea conocedor de la ubicación donde las va a instalar el cliente. El fabricante debe garantizar esto por medio de una declaración fehaciente. Las claves no modificables deben ser de aplicación únicamente en sistemas provistos de CAS de clase A.

5.1.7.1.9.2 Intercambio de claves

El intercambio de claves debe utilizar métodos asimétricos (basados en algoritmos tales como RSA o ECC), o simétricos (tales como Kerberos 5). Los mecanismos para el cambio de claves deben aportar, por lo menos, el mismo nivel de seguridad que los métodos de transmisión de datos. Para tener información sobre las longitudes apropiadas de las claves, y la equivalencia entre las longitudes de las claves simétricas y asimétricas, véase el documento NIST SP 800-57. Cuando el intercambio de claves se produzca de forma automática o manual, su frecuencia debe cumplir con el documento NIST SP 800-57.

5.1.7.1.9.3 Cambio de claves

El fabricante debe suministrar una instrucción de uso que explique el procedimiento y la frecuencia para los cambios de claves. Los cambios solo se deben poder realizar tras la introducción de un código autorizado. Si el cambio de clave se realiza fuera de banda (fuera de un método de comunicación previamente establecido), se debe tener en cuenta lo indicado en el apartado 5.1.7.1.7.

5.1.7.2 Seguridad de la unidad de entrada en sistema distribuido

5.1.7.2.1 Generalidades

Este requisito solo se debe cumplir si se transmiten datos relacionados con la seguridad.

5.1.7.2.2 Seguridad física

Toda unidad de entrada en un sistema distribuido debe cumplir con lo indicado en el apartado 5.1.5.4, incluso las cerraduras de clase A.

5.1.7.2.3 Seguridad de la información

La información relevante de seguridad debe introducirse solamente en las unidades de entrada fiables y dedicadas, de conformidad con el apartado 5.1.7.1. Los intentos no autorizados de acceso, a dichas unidades de entrada deben bloquear el uso normal de las mismas, por ejemplo activando mecanismos que borren o inutilicen los textos de las claves criptográficas (es decir una respuesta tipo *tamper* a la manipulación). Se debe cumplir al menos con los requisitos del nivel 3 de seguridad física conforme al apartado 4.5.1 del documento FIPS Pub 140-2.

5.2 Requisitos de seguridad

5.2.1 Códigos utilizables

El número mínimo de códigos utilizables cuando se ensaya según el apartado 8.2.1, para cada clase y tipo de CAS, debe ser el indicado en la tabla 1. El número mínimo de 25 000 códigos debe ser suficiente, para las cerraduras de clase A con llave mecánica, solo si la resistencia a la manipulación, requerida en la tabla 1, cumple con el apartado 8.2.2. A partir de 80 000 códigos o más y de conformidad con el anexo B, el ensayo de resistencia a la manipulación no debe realizarse para las CAS de clase A.

CAS con códigos paralelos: El número mínimo de códigos utilizables debe multiplicarse por el número de códigos paralelos posibles.

CAS con códigos de apertura de extensión variable: Para el cálculo de los códigos aceptables se debe utilizar el número más corto que la CAS pueda admitir como códigos de apertura.

No debe ser posible abrir una CAS mecánica accionada con llave mediante otras llaves adicionales, según se requiere en el ensayo definido en el apartado 8.2.1.3.

5.2.2 CAS función de apertura de emergencia

Una CAS con un dispositivo de prevalencia (por ejemplo una CAS que permita la apertura inmediata con un dispositivo mecánico (por ejemplo, una llave) debe clasificarse en base al sistema con menor grado de seguridad utilizado.

5.2.3 Resistencia a la manipulación

5.2.3.1 Límite de pruebas

El número máximo de intentos de apertura por hora que pueden realizarse debe cumplir con lo indicado en la tabla 1.

NOTA Las CAS con autentificadores mecánicos no están incluidas en la tabla 1 porque el tiempo empleado para cambiar los autentificadores limita suficientemente el número de intentos.

5.2.3.2 Manipulación

Los valores mínimos de resistencia, M, especificados en la tabla 1, deben superarse en al menos dos de las tres muestras a ensayar en los ensayos de resistencia a la manipulación, realizados según el apartado 8.2.2.

5.2.4 Resistencia al robo destructivo

En los ensayos donde se aplica una fuerza externa, según el apartado 8.2.3, deben superarse los valores mínimos de resistencia especificados en la tabla 1.

5.2.5 Resistencia al espionaje

5.2.5.1 Cualquier información introducida en una CAS electrónica debe resultar irreconocible al cabo de 30 s, después de dicha entrada, incluso si el código de apertura ha sido introducido sólo parcialmente.

5.2.5.2 Para las CAS de clase C y D el ángulo por encima del cual la información del código se pueda visualizar ópticamente no debe ser superior a 30º respecto del eje central tal y como se define en el apartado 8.2.4.

5.2.5.3 La introducción de códigos pulsando directamente sobre un teclado no se permite en las CAS de clase C y D. Esta limitación no aplica para los códigos de un solo uso.

5.2.5.4 Emisión comprometedora de señales:

No debe ser posible asociar información no cifrada de seguridad con las señales emitidas por una parte cualquiera de un componente del sistema distribuido. Respecto a las radiaciones comprometedoras, se debe prestar atención especial al sistema de transmisión a causa del acoplamiento de la radiación y/o las transmisiones inalámbricas.

5.2.6 Resistencia eléctrica y electromagnética

5.2.6.1 Las CAS electrónicas conectadas a la red eléctrica deben permanecer en condiciones normales de uso durante las variaciones de voltaje de la red, caídas de tensión y pequeñas interrupciones del suministro, cuando se ensayen según el apartado 8.2.5.5.

Ante una pérdida de tensión, cuando una CAS esté en la condición de asegurada, debe permanecer asegurada (véase 8.2.5.3).

Las CAS conectadas a la red deben ser capaces de permanecer aseguradas durante fallos de suministro eléctrico de hasta 12 h (véase 8.2.5.4).

5.2.6.2 Tras el ensayo de resistencia a descargas electrostáticas según el apartado 8.2.5.5, una CAS electrónica ensayada debe cumplir los requisitos de la tabla 2. Durante este ensayo las muestras no deben variar la condición de aseguramiento de la CAS durante más de 5 ms.

5.2.6.3 Durante el ensayo de resistencia de una CAS electrónica a los campos electromagnéticos irradiados según el apartado 8.2.5.8, se deben cumplir con los requisitos de la tabla 2.

5.2.6.4 Después del ensayo de resistencia de una CAS electrónica a breves Incrementos de Tensión según el apartado 8.2.5.6, por estar conectada a la red (y cualquier otro cable anexo de más de 10 m de longitud conectado a un equipo externo), deben cumplirse los requisitos de la tabla 2. Durante este ensayo la muestra no debe variar la condición de aseguramiento de la CAS durante más de 5 ms.

5.2.6.5 Tras el ensayo de una CAS electrónica ante un incremento del voltaje (según el apartado 8.2.5.7), se deben cumplir los requisitos de la tabla 2. Durante este ensayo las muestras no deben variar la condición de aseguramiento de la CAS durante más de 5 ms.

5.2.7 Resistencia a los factores físicos medioambientales

Todas las CAS deben ensayarse en cuanto a su resistencia a la vibración y al impacto según los apartados 8.2.6.1 y 8.2.6.2, en cuanto a su resistencia a la corrosión según el apartado 8.2.6.4, y todas las CAS electrónicas deben someterse al ensayo de inmersión según el apartado 8.2.6.3.

5.2.8 Resistencia a la temperatura

5.2.8.1 Frío

Las CAS electrónicas deben mantenerse en condición de uso normal tras ensayarse a una temperatura de -10 °C durante 16 h según se describe en el apartado 8.2.7.1.

5.2.8.2 Calor

Las CAS electrónicas deben mantenerse en condición de uso normal, tras ensayarse a una temperatura de +55 °C durante 16 h según se describe en el apartado 8.2.7.2.

Tabla 1 – Requisitos de seguridad para todas las CAS

Clase y tipo	Número mínimo de registros retenidos de eventos de apertura	Número mínimo de códigos utilizables para cada tipo de codificación		Número máximo de intentos por hora para cada tipo de medio de codificación		Resistencia a la manipulación M	Resistencia al robo con daños D
						Unidades de resistencia mínimas RU	Unidades de resistencia mínimas RU
		Codificación material	Codificación nemotécnica[b]	Cualquiera	Nemotécnico		
Clase A							
Electrónica	Ninguno	25 000	80 000	300		30	80
Mecánica	No aplicable	25 000	80 000	No aplicable		30	80
Clase B							
Electrónica	10 (para 3 usuarios)	100 000	100 000	100		60	135
Mecánica	No aplicable	100 000	100 000	No aplicable		60	135
Clase C							
Electrónica	50	1 000 000	1 000 000	30		100	250
Mecánica	No aplicable	1 000 000	1 000 000	No aplicable		100	250
Clase D							
Electrónica	500	3 000 000	3 000 000	10		620	500
Mecánica	No aplicable	3 000 000	3 000 000	10[a]		620	500

[a] Excluyendo las cerraduras accionadas con llave.
[b] El número mínimo de dígitos requeridos, sólo en el caso de cerraduras electrónicas, es seis (6).

Tabla 2 – Requisitos mínimos de resistencia eléctrica y electromagnética en las condiciones de ensayo especificadas

Resistencia ante los campos electromagnéticos de radio-frecuencia irradiados (Método de ensayo EN 61000-4-3)			
Condiciones del ensayo	**Clases de CAS**	**Condiciones de la cerradura** [a]	
	A y B	O [b]	FS [b]
	C y D	n.a.	O [b]
	Nivel de ensayo	3 [c]	4 [c]
Resistencia a las perturbaciones conducidas, inducidas por campos de radio-frecuencia (Método de ensayo EN 61000-4-6)			
Condiciones del ensayo	**Clases de CAS**	**Condiciones de la cerradura** [a]	
	A y B	FS [b]	
	C y D	O [b]	
	Nivel de ensayo	3	
Resistencia a las descargas electrostáticas, a las sobrecargas eléctricas momentáneas y a las ondas de choque de alta energía			
	Clases de CAS A, B, C y D	**Condiciones de la cerradura** [a]	
		O	**FS**
Nivel del ensayo	EN 61000-4-2	4	
	EN 61000-4-4		4
	EN 61000-4-5		4

[a] N = Operativa normal O = Operable FS = Fallo de seguridad
[b] Indica la situación en la que la CAS debería quedar, en el peor de los casos, después del ensayo.
[c] Banda de frecuencia desde 80 MHz a 2 GHz.

Tabla 3 – Condiciones del medio ambiente físico

Resistencia a las vibraciones (Método de ensayo EN 60068-2-6, resistencia por barrido)			
Clase de CAS	**Aceleración** ***g***	**Banda de frecuencia Hz**	**Ciclos**
A y B	1	10 a 150	10
C y D	2	10 a 150	10

5.3 Requisitos de fiabilidad

5.3.1 Tras ser sometida a 10 000 ciclos según el apartado 8.3.1, la CAS debe permanecer en su condición normal.

5.3.2 Las entradas de códigos introducidas por medio de un disco giratorio no deben desviarse del ajuste en más del 1% del total del intervalo de ajuste, tras el ensayo de códigos de entrada dinámica según el apartado 8.3.3.

5.3.3 Las CAS mecánicas de código variable deben permanecer en la condición normal de uso, después de haberse realizado 100 cambios de código según el apartado 8.3.2.

6 Documentación técnica

La siguiente documentación técnica debe acompañar a los elementos ensayados:

6.1 Planos detallados de construcción, con dimensiones y tolerancias.

6.2 El cálculo de códigos utilizables y todos los parámetros significativos para ese cálculo.

6.3 Características de los dispositivos de contención incluyendo:

– las dimensiones de la cabeza del pestillo o de cualquier otro elemento de bloqueo;

– la operativa de los elementos de aseguramiento durante el movimiento de la cabeza del pestillo o del elemento de bloqueo.

6.4 Todos los valores dimensionales necesarios para unir o conectar la CAS a dispositivos externos (por ejemplo dispositivos de entrada de códigos, medios a través de los cuales se accionan los mecanismos de bloqueo) incluyendo:

– la dimensión del orificio de entrada para el código (por ejemplo el ojo de la cerradura);

– la dimensión del huso, teclados fijos y marcadores giratorios;

– las(s) dimensión(es) y tipología de los conectores para cables.

6.5 Descripción detallada del procedimiento para activar y modificar los códigos, así como las precauciones a tener en cuenta.

6.6 Parámetros para la instalación.

6.7 Instrucciones para el funcionamiento.

6.8 Documentación de los programas (*software*) y del equipo (*hardware*) de la CAS electrónica, incluyendo:

– la estructura de los programas;

– los diagramas de la circuitería;

– el listado de los códigos de programación.

6.9 Descripción del método de programación utilizado para:

– memorizar códigos;

– extraer códigos de la memoria;

– proteger el acceso a los datos memorizados y al programa;

– evitar daños a la memoria;

– bloquear la manipulación.

6.10 Impreso de solicitud de la clase de cerradura de alta seguridad (CAS) que se pretende homologar.

7 Muestras para ensayo

7.1 Se deben aportar un mínimo de cuatro muestras de ensayo. Si se va a llevar a cabo el ensayo de resistencia a la manipulación, se deben aportar otras tres muestras de ensayo adicionales. Estas tres muestras adicionales deben tener sus códigos de apertura seleccionados al azar y estos códigos no deben ser conocidos por el equipo encargado del ensayo ni dados a conocer antes de realizarse el mismo.

El solicitante debe proporcionar las muestras para el ensayo de manipulación montadas en una chapa de acero con tapa según el apartado 8.1.3.

NOTA Las muestras para el ensayo de resistencia a la manipulación pueden tener valores dimensionales específicos dentro de los límites de la documentación técnica, seleccionados por el laboratorio encargado del ensayo.

7.2 Cada muestra de ensayo debe incluir todos los componentes significativos de seguridad de la CAS, concretamente:

– el dispositivo de entrada o lectura;

– la unidad de procesamiento;

– el dispositivo de cierre;

– el mecanismo de bloqueo;

– cualquier dispositivo de anulación o de apertura de emergencia;

– cualquier otro componente del que dependa la seguridad de la muestra.

7.3 Cuando las muestras de ensayo sean cerraduras mecánicas con llave, una muestra de ensayo debe tener dos llaves adicionales aparte de la llave original. Una de las llaves adicionales debe tener un diente intermedio con una altura **superior** en un paso al diente equivalente en la llave correcta; la otra llave adicional debe tener ese mismo diente con una altura **inferior** en un paso al diente equivalente en la llave correcta.

8 Métodos de ensayo

8.1 Generalidades

8.1.1 Generalidades

El objeto de los ensayos es determinar la seguridad y fiabilidad de las muestras que se ensayan. En los ensayos de seguridad el objetivo es desbloquear la muestra del ensayo o degradar su nivel de seguridad; en los ensayos de fiabilidad el objetivo es determinar si la muestra del ensayo continúa funcionando sin pérdida de su nivel de seguridad, tras la exposición a las condiciones del ensayo.

Las muestras de CAS mecánicas para el ensayo de resistencia a la manipulación (véase 8.2.2) pueden verse sometidas hasta un máximo de 1 000 ciclos de funcionamiento (véase 8.3.1) con anterioridad al ensayo de manipulación. Estas muestras no deben someterse a ningún otro ensayo previamente al ensayo de manipulación.

Los ensayos para los requisitos criptográficos se basan en el estudio de la descripción del sistema proporcionado por el fabricante la cual debe incluir una lista de las normas referenciadas.

8.1.2 Evaluación por inspección

Todos los requisitos indicados en el apartado 5.1 deben evaluarse mediante inspección.

8.1.3 Procedimiento de ensayo

Se simula la utilización en una unidad de almacenamiento de seguridad montando las muestras de ensayo, de acuerdo con las instrucciones del fabricante, sobre una chapa y una cubierta de acero, ambas sin ningún otro orificio que no sean los necesarios para el montaje de acuerdo con la documentación técnica (véase el capítulo 6) y la figura 1, para los siguientes ensayos: resistencia a la manipulación (véase 8.2.2), resistencia al robo con daños (véase 8.2.3), resistencia al espionaje (véase 8.2.4), y resistencia eléctrica y electromagnética (véase 8.2.5).

En el caso de llevar a cabo la entrada dinámica de códigos mediante equipamiento cíclico, no debe ser necesario emplear una unidad de almacenamiento de seguridad simulada (maqueta).

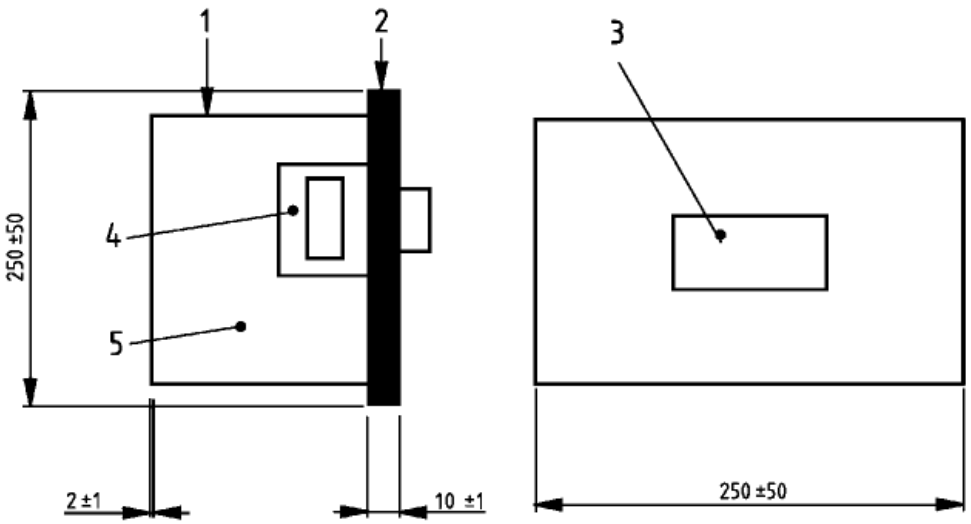
Se permite el acceso a la muestra de ensayo de acuerdo con la documentación técnica del capítulo 6. Cuando la muestra de ensayo sea una CAS electrónica, la cubierta debe ser de acero y estar unida a la chapa de acero por tornillos con una separación entre ellos de al menos de 50 mm en los cuatro lados de la chapa de acero.

Se realizan los ensayos de resistencia a la manipulación (véase 8.2.2), el ensayo de resistencia al robo con daños (véase 8.2.3) y el ensayo de resistencia al espionaje (véase 8.2.4), únicamente en aquellas partes de la muestra de ensayo accesibles cuando está montada en la chapa de acero, y sin perforar a la fuerza ni la chapa de acero ni la cubierta.

El ensayo de robo no debe incluir ningún ataque a la caja de la cerradura o su tapa (cubierta), desde el interior de la cerradura que cause desperfectos en cualquier elemento de la caja o la tapa, y/o las desmonte parcial o totalmente.

Cuando la situación de CAS asegurada deba monitorizarse, la comprobación ha de hacerse con una exactitud de 5 ms.

Medidas en milímetros



Leyenda
1 Cubierta de acero
2 Placa de montaje de acero
3 Dispositivo de lectura
4 Cerradura
5 Cubierta

NOTA La cubierta de acero debe estar a una distancia mínima de la cerradura de 20 mm.

Figura 1 – Diseño esquemático de la cubierta y su montaje

8.2 Ensayos de seguridad

8.2.1 Códigos utilizables

8.2.1.1 Se evalúa el número de códigos utilizables (véase 6.3) declarado por el fabricante para verificar que resulta correcto.

8.2.1.2 Para calcular el número de códigos utilizables por una CAS de combinación mecánica, se utiliza el procedimiento del siguiente ejemplo y el mecanismo de ensayo cíclico:

a) los discos de codificación, a excepción del último en ajustarse, se alinean en sus números de apertura;

b) a continuación se ajusta el último disco codificador para el número del ensayo, empezando con su número de apertura menos 5 dígitos;

c) se comprueba si la cerradura se abre. En caso de apertura, se registra el número más bajo, N mín. y el número más alto, N máx.;

d) se incrementa el número del ensayo en 0,25 dígitos;

e) se repiten los pasos del a) al d) hasta que el número del ensayo sea el número de apertura más 5 dígitos.

La tolerancia de entrada de códigos es T = N máx. - N mín.

El número de códigos utilizables es:

En cerraduras de 3 discos: $Cn = (D1/T) \times (D2/T) \times (D3/T)$

es decir $(100/1,75) \times (100/1,75) \times (80/1,75) = 149\ 271$

En cerraduras de 4 discos: $Cn = (D1/T) \times (D2/T) \times (D3/T) \times (D4/T)$

es decir $(100/1,75) \times (100/1,75) \times (100/1,75) \times (80/1,75) = 8\ 529\ 779$

Dx = número de dígitos en el disco de codificación multiplicado por menos la zona secreta declarada por el fabricante (normalmente en el último elemento de codificación en ajustarse).

8.2.1.3 Para las cerraduras mecánicas de llave deben utilizarse las llaves que tengan un diente con una diferencia de altura de un paso (véase 7.3), con un par de torsión máximo de 1,5 Nm para determinar si cualquiera de ellas abre la muestra.

8.2.1.4 Para ensayar la resistencia de la llave, la cerradura debe instalarse sobre un soporte conforme a la figura 1. Entonces, se debe introducir por completo la llave correspondiente en la cerradura y se debe incrementar progresivamente el par hasta $(2,5 \pm 0,1)$ Nm durante 5^{+1}_{0} s. Después, debe ser posible retirar la llave de la cerradura y volverla a utilizar para accionar la misma cerradura con un par igual o inferior a 1,5 Nm.

8.2.2 Resistencia a la manipulación

8.2.2.1 Principio

Las muestras de ensayo y la documentación técnica (véase el capítulo 6) se examinan y se decide el método de evaluación de la resistencia a la manipulación de acuerdo con las siguientes especificaciones:

Las CAS mecánicas de clase A, con 80 000 códigos utilizables y que cumplen los requisitos de diseño del Anexo B, no deben ensayarse para determinar su resistencia a la manipulación.

Las CAS mecánicas de clase B que cumplen los requisitos de diseño del anexo B no deben ensayarse a menos que el laboratorio encargado del ensayo no tenga la certeza de que se satisfacen los requisitos de resistencia a la manipulación (véase la tabla 1).

Las CAS electrónicas de todas las clases y las CAS mecánicas de clases C y D deben ensayarse para determinar su resistencia a la manipulación.

Las CAS mecánicas de las clases A y B, que no cumplan con los requisitos de diseño del anexo B, o las que no puedan demostrar que los cumplen, pueden ensayarse, para determinar su resistencia a la manipulación, a petición del solicitante. En la determinación de si se satisfacen los requisitos de resistencia a la manipulación, el resultado del ensayo debe prevaler sobre la evaluación de tolerancias.

8.2.2.2 Equipos

8.2.2.2.1 Reloj que mida horas, minutos y segundos.

8.2.2.2.2 Herramientas según los criterios de la tabla 4.

8.2.2.3 Procedimiento

Se examina un número suficiente de muestras de ensayo (según el capítulo 7) junto con la documentación técnica (véase 6.2) y el anexo B, y se diseña un programa de ensayos de manipulación utilizando las herramientas (véase la tabla 4), que deben ser las que con más probabilidad, en opinión del equipo de ensayo, se obtendrían los resultados menores de los valores de resistencia. Se realiza un examen preliminar de las muestras no selladas (según capítulo 7) y se llevan a cabo todas las pruebas, tomándose las medidas necesarias para determinar qué métodos se deben emplear para intentar abrir la CAS mediante su manipulación.

8.2.2.4 Se manipula cada una de las tres muestras de ensayo selladas una vez utilizando el procedimiento de ensayo de manipulación según apartado 8.2.2.3. Se mide el tiempo de manipulación, dando por finalizado el ensayo cuando el valor de resistencia a la manipulación M, para dicha clase de CAS (véase la tabla 1), haya sido superado.

8.2.2.5 Expresión de resultados

Se calcula el valor de resistencia a la manipulación, M, según la siguiente fórmula:

$$M = t + B$$

donde

t es el tiempo empleado en abrir la muestra de ensayo, expresado en minutos;

B es el valor de unidad básica, y es uno de los dos valores (0 o 15 según la tabla 4) adecuados para la categoría más alta de las herramientas utilizadas;

M es el valor de resistencia a la manipulación, expresado en unidades de resistencia (RU).

Tabla 4 – Lista de herramientas para el ensayo de resistencia a la manipulación de las CAS mecánicas y electrónicas

Número	Nombre de la categoría	Unidades básicas	Descripción	Ejemplos mecánicos	Ejemplos electrónicos
1.	Herramientas de fácil adquisición, herramientas manuales e instrumentos	0	Herramientas o materiales de fácil adquisición para cualquier persona en ferreterías. Las herramientas son lo suficientemente pequeñas para ser llevadas sin ser detectadas. No se necesita ninguna habilidad para su uso efectivo. No necesitan corriente eléctrica y no producen ruidos tales que puedan llamar la atención.	Destornilladores	Voltímetros
				Alicates	Amperímetros
				Tenacillas	Soldador
				Lima	Cableados
				Pinzas	Medidor de fases
				Punzones	Ordenador personal
				Martillos	Baterías
				Artículos de medición	Suministro eléctrico
				Lupas	
2.	Herramientas para la apertura de una CAS	15	Cualquier herramienta o instrumento para la apertura de CAS que pueda adquirirse en compañías de suministro de herramientas para especialistas y disponibles sólo para cerrajeros profesionales, o bien que están especialmente diseñadas, fabricadas o modificadas. Para su uso efectivo se necesitan habilidades especiales y un conocimiento detallado de las CAS y de los métodos de apertura de las mismas. Puede darse el caso de que esas herramientas sean altamente especializadas y efectivas con un único tipo de CAS.	Herramientas de forzamiento	Analizador de espectro
				Recambios de cerradura	Osciloscopio
				Llaves vírgenes (no labradas)	Equipo de amplificación de sonido
				Llaves de prueba	Fibra óptica
				Equipo de amplificación de sonido	Detectores de radiación electromagnética
				Sondas ópticas o de fibra óptica	Máquinas de apertura automática
				Dispositivo de marcado giratorio	

8.2.3 Resistencia al robo con daños

8.2.3.1 Principio

Se examinan las muestras de ensayo y la documentación técnica (véase el capítulo 6), desarrollando e implementando un método para la evaluación de la resistencia al robo con daños.

8.2.3.2 Equipos

8.2.3.2.1 Reloj que mida horas, minutos y segundos.

8.2.3.2.2 Herramientas de la categoría A según la Norma EN 1143-1.

8.2.3.2.3 Herramientas de acuerdo con los criterios de la tabla 4.

8.2.3.3 Procedimiento

Se examinan la(s) muestra(s) de ensayo junto con la documentación técnica (véase el capítulo 6) y se llevan a cabo todas las pruebas, tomando las medidas necesarias, para decidir el método y las herramientas que proporcionarán el valor más bajo de resistencia al robo con daños. Se ensaya una muestra sellada y se registra el tiempo del ensayo. Se puede dar por concluido el ensayo cuando el valor de resistencia al robo con daños, de la clase a la que corresponde la muestra (véase la tabla 1), haya sido superado.

8.2.3.4 Expresión de resultados

Se calcula el valor de resistencia al robo con daños, D, según la siguiente fórmula:

$$D = 5\,t + \Sigma\,B\,V + B$$

donde

D es el valor de resistencia al robo con daños, en unidades de resistencia (RU);

t es el tiempo empleado en abrir la muestra de ensayo, expresado en minutos;

Σ B V es la suma de los valores básicos de todas las herramientas utilizadas de categoría A, según la Norma EN 1143-1.

B tiene un valor de 0 o 15, de acuerdo con el valor de unidad básica más alto de cualquiera de las herramientas utilizadas según la tabla 4.

8.2.4 Resistencia al espionaje

8.2.4.1 Principio

Se monta la muestra de ensayo de acuerdo con la figura 1 y se pone en vertical a una altura adecuada para observar cualquier posición de la CAS, desde donde se pueda ver el código de entrada.

Los ensayos se realizan con objeto de reconocer la información de entrada.

Se apoyan dos pantallas sobre la muestra de ensayo para limitar el ángulo de espionaje.

Las pruebas de espionaje se realizan para determinar si cualquier información de entrada es reconocible desde fuera del ángulo determinado por las pantallas referidas.

8.2.4.2 Equipos

8.2.4.2.1 **Plataforma de pruebas** capaz de mantener en posición vertical la muestra de ensayo montada.

8.2.4.2.2 **Reloj** que mida horas, minutos y segundos.

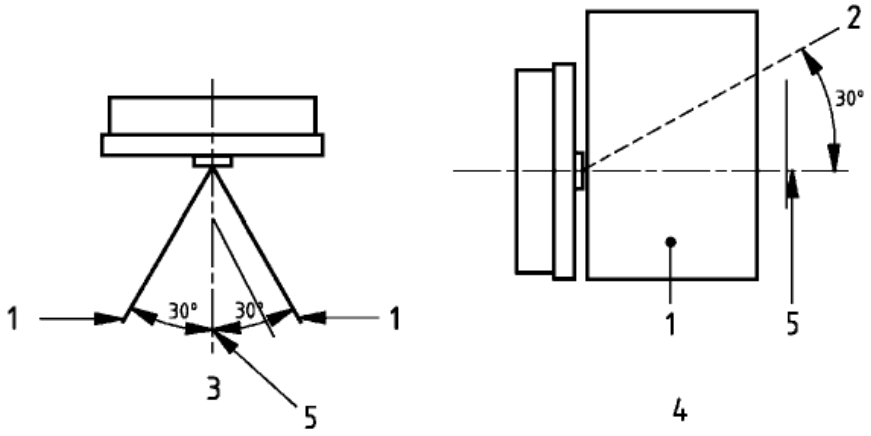
8.2.4.2.3 **Dos pantallas** capaces de definir un ángulo de espionaje limitado.

Para las CAS de clase C y D puede ser necesario realizar el ensayo de espionaje con distintas condiciones de iluminación.

8.2.4.3 Procedimiento

8.2.4.3.1 Se utiliza una CAS electrónica y se introduce el código de apertura. Se observa si la información de entrada es irreconocible 30 s después de la introducción del último dígito. El ensayo se realiza introduciendo en primer lugar el código completo y después solamente parte del mismo.

8.2.4.3.2 Se colocan dos pantallas (véase 8.2.4.2.3) delante de la muestra de ensayo, formando un ángulo de 60º, de acuerdo con la figura 2, y cuando se introducen los códigos se evalúa si pueden ser reconocidos, desde un ángulo de 30º en vertical situada en el eje central de la muestra.



Leyenda
1 Pantalla
2 Ángulo de visibilidad
3 Planta
4 Alzado
5 Línea central

Figura 2 – Dos diagramas esquemáticos de la planta y el alzado del equipamiento para el ensayo de espionaje

8.2.5 Resistencia eléctrica y electromagnética

8.2.5.1 Principio

Se ensaya la resistencia eléctrica y electromagnética, de las muestras de ensayo de las CAS electrónicas, en condiciones normales antes de cada ensayo de acuerdo con la tabla 2. A partir de la clase B se debe incluir también un ensayo de pérdida de corriente y de influencia sobre el suministro eléctrico, según el apartado 8.2.5.3.

8.2.5.2 Procedimiento

Se ensayan las muestras de acuerdo con los requisitos del apartado 5.2.6 y se evalúa la CAS después de cada ensayo para determinar si continúa en su estado normal, funcionando o en situación de fallo de seguridad, cumpliendo con los requisitos.

8.2.5.3 Ensayos de pérdida de corriente y de influencia del suministro eléctrico

Se coloca la muestra de ensayo en la condición de asegurada y se corta la corriente. Se evalúa si continúa en condición de asegurada.

Después de ello, se ensaya si es posible un desbloqueo no intencionado vía suministro eléctrico mediante un incremento constante de 0 V a 220 V con corriente continua o corriente alterna, estando la cerradura conectada a cables externos accesibles.

8.2.5.4 Aseguramiento durante el corte en el suministro eléctrico

Se coloca una muestra de ensayo de CAS conectada a la red en la posición de no asegurada. Se corta la corriente. Se evalúa si la CAS puede ser asegurada 12 h después de haberse cortado la corriente.

8.2.5.5 Descarga electrostática

Se llevan a cabo ensayos de descarga electrostática de acuerdo con la Norma EN 61000-4-2, utilizando los niveles de ensayo de la tabla 2, para las partes de la muestra del ensayo de la CAS con las que el usuario entra en contacto físico durante cualquier operación, por ejemplo introducción del código, desbloqueo, bloqueo o cambio de código. La polaridad de la placa de montaje es + o –, por lo tanto ambas polaridades deben ensayarse. Para este ensayo puede quitarse la cubierta (véase 8.1.3).

Para las CAS que vayan a ser montadas en cajas fuertes sin bastidor de metal adicional, se pueden realizar ensayos adicionales a las muestras de ensayo sin montaje o en un montaje no conductivo, sin que estos ensayos formen parte del esquema de clasificación.

8.2.5.6 Interrupciones breves del voltaje eléctrico

Se ensayan las cerraduras alimentadas eléctricamente de acuerdo con la Norma EN 61000-4-4, utilizando los niveles de ensayo de la tabla 2.

8.2.5.7 Inmunidad al sobrevoltaje

Se ensaya de acuerdo con la Norma EN 61000-4-5, utilizando los niveles de ensayo de la tabla 2.

Las muestras de ensayo de CAS pueden ensayarse en primer lugar para el nivel más alto. Si estos niveles elevados se resisten, el ensayo para los niveles inferiores no debe llevarse a cabo.

8.2.5.8 Campos electromagnéticos radiados

Se ensaya de acuerdo con las Normas EN 61000-4-3 y EN 61000-4-6, utilizando los valores de ensayo de la tabla 2.

8.2.5.9 Expresión de resultados

Se evalúa si se produce algún cambio en la condición de seguridad de la muestra de CAS, o si permanece en condición de seguridad, tanto durante como después del ensayo, de acuerdo con la tabla 2.

8.2.6 Resistencia al medioambiente físico

8.2.6.1 Vibración

Se ensaya la resistencia a la vibración de las muestras de CAS, que están en condición operativa, sobre cada uno de los tres ejes x, y y z, de acuerdo con la Norma EN 60068-2-6, utilizando los valores de ensayo de la tabla 3.

Método de ensayo: (1) Resistencia por barrido

(2) Diez (10) ciclos

Tras la exposición a las vibraciones, la muestra de ensayo debe continuar operativa y asegurada.

8.2.6.2 Ensayo de resistencia al impacto

8.2.6.2.1 Generalidades

Durante el ensayo debe haber una monitorización continua (véase 5.2.7) para comprobar si el aseguramiento de la muestra ensayada se mantiene por más de 5 ms. También se evalúa si la muestra del ensayo continúa en condiciones operativas después de exponerse al ensayo con cinco caídas de $50^{0}_{-5}\ g$.

8.2.6.2.2 Principio

Las muestras de CAS se dejan caer desde una altura de 1 m para provocar choques por impacto. Se realizan 5 caídas sobre un eje a elección del encargado del ensayo. Tras cinco caídas con 50^{0}_{-5} *g*, se evalúa la condición de la muestra (véase 5.2.7). En función del diseño de la cerradura, el laboratorio de ensayo puede decidir realizar ensayos adicionales, con un máximo de 50 impactos de más de 50 *g* utilizando el mismo equipo.

8.2.6.2.3 Equipo

Un banco de pruebas que permita a la muestra del ensayo, una vez montada en una placa rígida de acuerdo con el método especificado en la documentación técnica (véase el capítulo 6), caer verticalmente desde (1 000 ± 5) mm y ser frenada. La desaceleración se mide en la placa de montaje, y solo esta placa será la que contacte con cualquier parte del banco de pruebas.

8.2.6.2.4 Procedimiento

a) Se prepara la muestra de ensayo de tal forma que el elemento de bloqueo se encuentre en posición de CAS asegurada.

b) Se eleva la muestra de ensayo para permitirle una caída de 1 000 mm ± 5 mm.

c) Se realizan cinco (5) impactos con 50^{0}_{-5} *g* con el eje y dirección escogidos, y se evalúa si se satisface la condición de aseguramiento;

d) Si se considerase necesario se realizan impactos adicionales, con más de 50 *g*, utilizando el mismo material de ensayo.

8.2.6.2.5 Expresión de resultados

Se registra la condición de la muestra de ensayo tras el ensayo de impacto. Después de la exposición a impactos adicionales, de más de 50 *g*, la muestra de ensayo no tiene porque mantenerse en condición operativa, pero sí en condición asegurada.

8.2.6.3 Ensayo de inmersión

Se ensaya la CAS electrónica, en condiciones operativas y según la Norma EN 60068-2-17:1994, ensayo Qf, sumergiendo la unidad procesadora y el mecanismo de cierre a una profundidad de 1 m durante 30 min o hasta que el líquido dieléctrico entre en contacto con la unidad procesadora. La CAS no se debe abrir salvo que se opere intencionadamente.

8.2.6.4 Ensayo de corrosión

Tras ser ensayada contra la corrosión habiendo sido expuesta a tres ciclos (8 h de exposición a SO_2 y 16 h a la atmósfera ambiente), de conformidad con la Norma EN ISO 6988, la CAS debe mantenerse operativa. Este ensayo se realiza con la CAS completa, pero con posibilidad de retirar las pilas.

8.2.7 Ensayo de resistencia a la temperatura

8.2.7.1 Frío

Se ensaya la CAS electrónica, que se encuentra en condición normal, durante 16 h a -10 °C, de conformidad con la Norma EN 60068-2-1:2007, ensayo Ab. Tras el ensayo, cuando la muestra haya alcanzado una temperatura de al menos +5 °C, se registra la condición de la misma.

8.2.7.2 Calor

Se ensaya la CAS electrónica, que se encuentra en condición normal, durante 16 h a 55 °C de conformidad con la Norma EN 60068-2-2:2007, ensayo Bb. Se registra la condición de la muestra inmediatamente después del ensayo y antes de que se haya enfriado por debajo de 45 °C.

8.3 Ensayo de fiabilidad

8.3.1 Ciclos

8.3.1.1 Principio

Una determinada muestra de ensayo CAS en condición normal antes de cada ensayo, debe ser repetidamente sometida al siguiente ciclo de ensayos: introducción de código, desactivado de la seguridad, apertura, cierre, activado de la seguridad.

Para las CAS electrónicas, el ensayo de fiabilidad de las unidades de lectura se puede realizar por separado de la unidad procesadora y del mecanismo de cerrado. En este caso, el fabricante puede modificar los programas para posibilitar la realización del ensayo por separado.

8.3.1.2 Equipo para el ensayo cíclico

El equipo se ha diseñado especialmente para permitir la introducción del código de apertura y realizar el desbloqueo, el bloqueo y la activación de la seguridad. También puede permitir el cambio de código.

8.3.1.3 Procedimiento

Se somete la muestra de ensayo al número de ciclos definidos en el apartado 5.3.1. Durante el ensayo, el pestillo debe exponerse a una carga de 2,5 N, mientras se realizan 5 000 ciclos con la carga en sentido contrario a la extensión del pestillo y 5 000 ciclos en el sentido de extensión del pestillo.

8.3.1.4 Expresión de resultados

Se evalúa y registra la condición de la CAS.

8.3.2 Cambio de códigos

8.3.2.1 Principio

Una muestra de ensayo de CAS en condición normal, se somete de forma cíclica al siguiente procedimiento de cambio de código:

– inserción de un código válido;

– procedimiento de cambio de código, por ejemplo insertar/girar una llave de cambio en una cerradura de combinación mecánica;

– inserción de un código nuevo;

NOTA Para algunas CAS electrónicas será necesario repetir la inserción del código.

– ajuste del nuevo código, por ejemplo girar/retirar la llave de cambio en una cerradura de combinación mecánica;

– accionamiento de la cerradura con el nuevo código al menos tres veces.

La secuencia de cambio de código puede llevarse a cabo manualmente, o bien utilizando un aparato de ensayo de funcionamiento cíclico (véase 8.3.1.2).

8.3.2.2 Procedimiento

Se somete a la muestra de ensayo al número de cambios de código especificados en el apartado 5.3.3.

8.3.2.3 Expresión de resultados

Se evalúa y registra la condición de la CAS.

8.3.3 Introducción del código dinámico de una CAS de combinación mecánica

8.3.3.1 Principio

La muestra de ensayo empleada en el ensayo de ciclos y en condición normal, es sometida a condiciones cíclicas de aceleración, velocidad y desaceleración.

8.3.3.2 Equipo

Equipo especialmente diseñado para la entrada repetida de códigos, mediante aceleración y velocidad controladas.

8.3.3.3 Procedimiento

8.3.3.3.1 Se toma la muestra, utilizada para el ensayo de ciclos (véase 8.3.1), y se hace girar el mecanismo 6 vueltas a la velocidad de 10 rad/s, en una determinada dirección.

Si la CAS no se desbloquea, se introducen otros códigos que se encuentren dentro del margen del uno por ciento del rango del código de apertura original y se evalúa si la CAS se abre.

8.3.3.3.2 Se toma la muestra de ensayo, utilizada en el anterior apartado 8.3.3.3.1, y se introduce el código de apertura con una rotación de 10 rad/s, y se desacelera desde 800^{+300}_{-100} rad/s^2 hasta velocidad cero. Se verifica si la cerradura se desbloquea.

8.3.3.4 Expresión de los resultados

Se evalúa y registra si la cerradura se desbloquea.

9 Informe de ensayo

9.1 Se adjudica un número de identificación único al informe del ensayo.

9.2 Se informa sobre los siguientes datos:

- el nombre del fabricante, el lugar y el año de fabricación;
- la documentación técnica aportada de acuerdo con el capítulo 6;
- la identificación por el fabricante de las muestras de ensayo;
- la fecha y lugar del ensayo;
- los resultados de los ensayos, incluyendo las descripciones de los métodos empleados, las herramientas utilizadas y los cálculos referentes a manipulación y robo con daños;
- la clasificación obtenida, durante la evaluación conforme a esta norma europea.

10 Marcado

Toda CAS debe estar identificada de forma legible e inalterable en lugar visible, siempre que se instale en una unidad de almacenamiento de seguridad.

La identificación debe incluir como mínimo lo siguiente:

a) la identificación del fabricante;

b) el número del modelo;

c) el año de fabricación;

d) la clasificación;

e) el número de esta norma europea.

Si la clase de resistencia de la CAS variase como consecuencia del tipo de unidad de entrada de códigos instalada con la cual está asociada, esta información debe marcarse en la CAS.

Anexo A (Normativo)

Parámetros para instalación e instrucciones de uso

A.1 Instrucciones de instalación

La seguridad global de una CAS depende del método de instalación, por lo que el fabricante debe proporcionar toda la información necesaria para una correcta instalación.

Los parámetros para la instalación incluyen lo siguiente:

- las dimensiones de la cabeza del pestillo u otros componentes del bloqueo;
- el desplazamiento del mecanismo de bloqueo, por ejemplo el de la cabeza del pestillo desde la posición de cerrado a la de abierto;
- la fuerza que se puede ejercer sobre el mecanismo de bloqueo al menos durante 10 000 ciclos;
- los elementos materiales de la unidad de almacenamiento de seguridad a los que se puede fijar la cerradura;
- las referencias marcadas para instalar los tornillos de fijación con indicación de las posibles roscas;
- la información sobre los tornillos de fijación que pueden utilizarse (roscas, longitud, material, resistencia, o en su caso, utilización de tornillos suministrados);
- el par de apriete máximo recomendado para los tornillos de fijación;
- las recomendaciones para el bloqueo de los tornillos (arandelas, arandelas de bloqueo o pegamento);
- la posición y la forma, así como la dimensión mínima y máxima de los agujeros para la llave, ejes de dial y cableado;
- los elementos de condenación recomendados para la pestillería;
- otros datos sobre la carga del pestillo de la cerradura;
- las recomendaciones para la protección de las cerraduras contra ataques destructivos;
- los parámetros de montaje (ejes de dial, chavetas…) para las cerraduras mecánicas de combinación;
- la información sobre cómo deben instalarse los contactos del pestillo, en las cerraduras electrónicas, si ello fuese de aplicación;
- la posible recomendación para que los elementos de seguridad de la CAS no sean accesibles a personas no autorizadas cuando la puerta de la unidad de almacenamiento de seguridad donde se está instalada se encuentre abierta.

El laboratorio puede proporcionar una lista de puntos sensibles o previsiblemente débiles como información a utilizar durante los ensayos de robo de la caja fuerte o puerta de la cámara acorazada (véase la Norma EN 1143-1) (opcional).

A.2 Instrucciones operativas

Las instrucciones operativas deben contener todos los aspectos importantes para el usuario/operador, de forma clara y entendible.

Deben incluirse las siguientes instrucciones:

a) Generalidades

1) Recomendaciones de seguridad sobre como custodiar llaves, tarjetas, activadores, etc.

b) Cerraduras con llave

1) La llave debe retirarse de inmediato después de toda operación de apertura y cierre, de forma que ninguna persona no autorizada pueda tener acceso a la misma.

2) En caso de pérdida de una llave, la cerradura debe sustituirse de inmediato o el código cambiado por uno nuevo.

c) Cerraduras con código

1) El código de fábrica debe cambiarse por el usuario final en cuanto la CAS se ponga en servicio.

2) No se deben utilizar códigos simples que resulten fáciles de adivinar (por ejemplo 1, 2, 3, 4, 5, 6).

3) No se deben utilizar códigos que reflejen información personal (por ejemplo cumpleaños) u otros datos que puedan ser fácilmente relacionables con el usuario final.

4) Tras un cambio de código, la cerradura debe probarse varias veces con la puerta de la unidad de almacenamiento de seguridad abierta.

Solo aplicable para códigos de cerraduras mecánicas de combinación: cuando se alcance la condición de CAS asegurada (3.23), las piezas portadoras del código deben colocarse aleatoriamente.

d) Activadores electrónicos

1) La transmisión de la clave criptográfica durante el proceso de inicialización debe realizarse por personal autorizado en un entorno seguro.

2) Qué información relevante de seguridad se almacena sin encriptar, si fuese de aplicación.

3) Si el activador electrónico no está protegido contra multi-usos, la siguiente instrucción debe incluirse en el manual: Nunca utilizar este activador electrónico en aplicaciones diferentes a este modelo de CAS.

e) Sistemas distribuidos

1) Procedimiento y frecuencia para realizar los cambios de claves/llaves.

Anexo B (Normativo)

Determinación de la resistencia a la manipulación debida a los requisitos del diseño

B.1 Generalidades

Estos criterios para requisitos del diseño se reconocen como buenos indicadores de la resistencia a la manipulación de algunos diseños específicos de CAS. Se ha adquirido suficiente experiencia para permitir identificar y cuantificar los criterios de diseño que afectan a la resistencia a la manipulación. Para otros diseños, aún no se pueden dar los criterios críticos, pero después de que se hayan realizado suficientes ensayos, tales criterios podrán ser establecidos. Dicha información, cuando esté disponible, se incluirá en una futura revisión de esta norma.

B.2 Cerraduras de llaves

B.2.1 Generalidades

El mecanismo de identificación del código en este ejemplo de CAS con cierre de llave, implica la introducción de un componente del pasador en las gorjas directrices cuando se alinean correctamente. Para estas cerraduras, su resistencia a la manipulación depende de cierta tolerancia dimensional y de las características de diseño de las gorjas, el conjunto de gorjas y el pasador.

Las CAS de cierre de llave de clase A y B, que cumplen con los criterios indicados en los apartados B.2.2, B.2.3 y B.2.4 y con los requisitos de diseño del apartado B.2.5 pueden considerarse suficientemente resistentes a la manipulación (véase la tabla 1) y por lo tanto no es necesario el ensayo para evaluar dicha resistencia.

B.2.2 Margen de seguridad de la ranura de la gorja

La diferencia entre la anchura de la ranura de la gorja y la anchura de la parte del pasador que entra en la ranura de la gorja durante la apertura, no debe exceder de la mitad del desplazamiento de la gorja provocado por un incremento de la altura de alzada. Es decir:

$$C \leq \frac{H}{2}$$

donde

C es la diferencia entre la anchura de la ranura de la gorja y la del pasador, calculados según la fórmula reseñada a continuación;

H es el desplazamiento en la entrada de la gorja causado por un incremento de una altura de alzada (véase la figura B.1).

Se debe calcular C y establecer una tolerancia para los radios de encuentro (véase la figura B.2) sobre la ranura de la gorja y el pasador de la siguiente manera:

$$C = S2 - S1 + 0{,}3\ (R1 + R2 + R3 + R4)$$

donde

S1 es el valor mínimo de anchura del pasador que cumple con las dimensiones nominales y tolerancias indicadas en los planos del fabricante. Si la anchura del pasador no es uniforme, S1 debe ser la anchura en el punto donde finalizan los radios de encuentro R3 y R4;

S2 es la anchura a la que finalizan los radios de encuentro R1 y R2. Si la ranura de la gorja no está en paralelo, véase la figura B.3 para determinar el valor S2;

R1, R2, R3 y R4 son los valores máximos de los radios de encuentro de la gorja y el pasador que cumplen con las dimensiones nominales y tolerancias consignadas en los planos del fabricante.

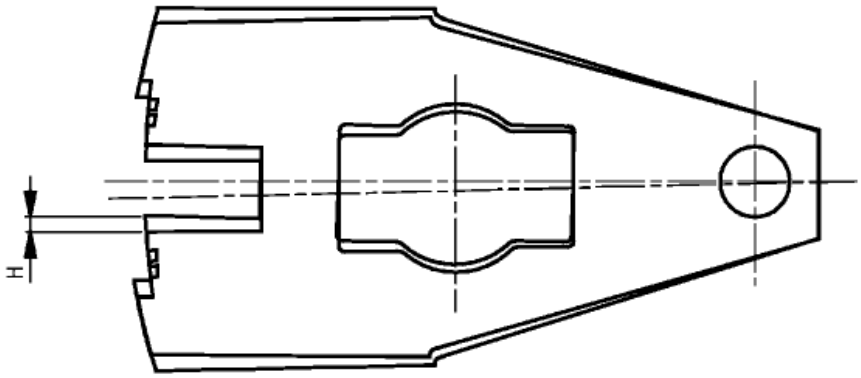
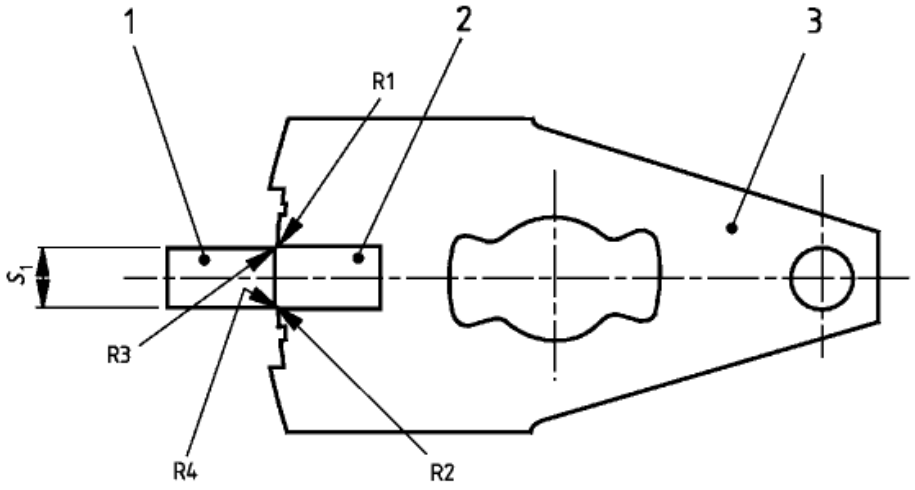


Figura B.1 – Diagrama esquemático que ilustra el desplazamiento de la gorja causado por el incremento de una altura de alzada



Leyenda
1 Pasador
2 Ranura de entrada
3 Gorja

Figura B.2 – Diagrama esquemático que ilustra los radios de encuentro de la entrada de la ranura de la gorja y el pasador

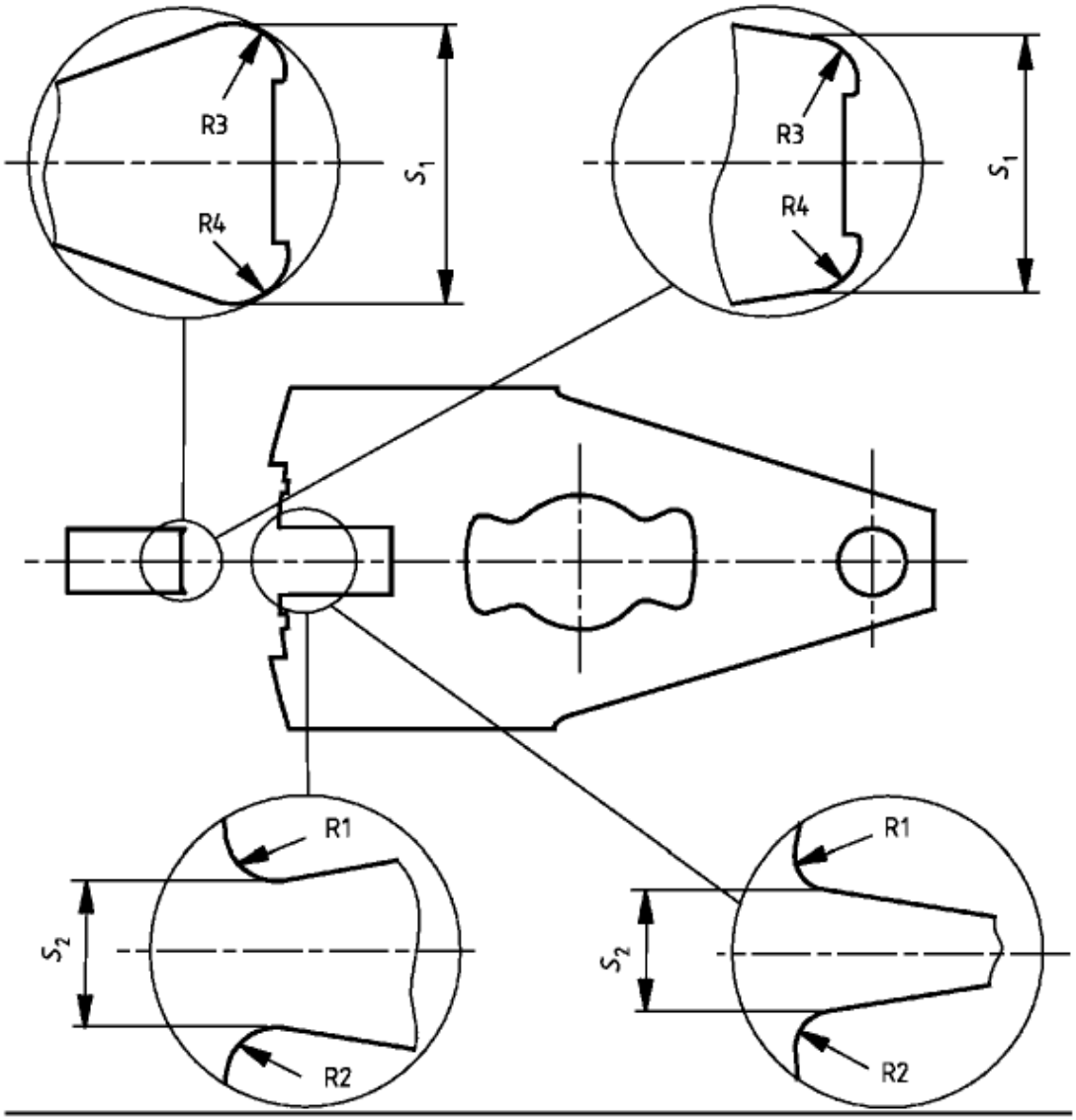
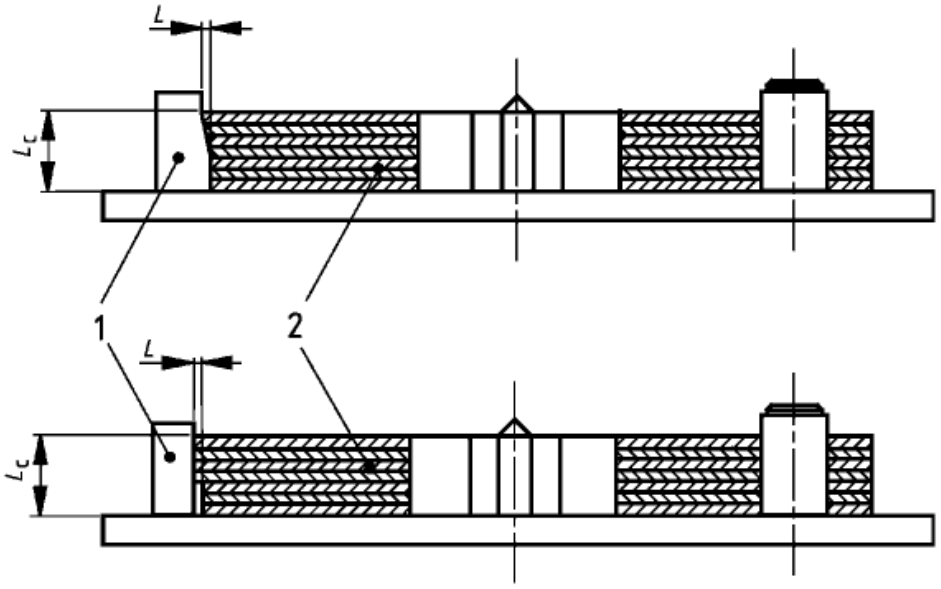


Figura B.3 – Diagrama esquemático destacando los radios de encuentro en el punto de entrada de la ranura de la gorja y el frente de entrada del pasador



Leyenda
1 Pasador
2 Gorjas

Figura B.4 – Diagrama esquemático que ilustra la separación entre el pasador y las gorjas

B.2.3 Pasador

Cuando el pasador esté en contacto con cualquier gorja la separación entre el pasador y cualquier otra gorja (véase la figura B.4) debe satisfacer la siguiente ecuación:

$$L \leq \frac{L_c}{50}$$

donde

L es la separación máxima entre el frente de entrada del pasador y la superficie de cualquier gorja (siendo esas partes de la gorja, cualquiera menos la ranura y la falsa ranura, las cuales podrían entrar en contacto con el frente de entrada del pasador);

L_c es la anchura del conjunto de gorjas.

B.2.4 Falsas ranuras

Las gorjas de las cerraduras con llaves de clase A y B deben tener falsas ranuras (véase la figura B.5). Para las cerraduras de clase B, las posiciones de las falsas ranuras deben corresponder a las posiciones de la ranura de entrada. Los márgenes de seguridad del pasador no deberían diferir de los de las falsas ranuras en las gorjas.

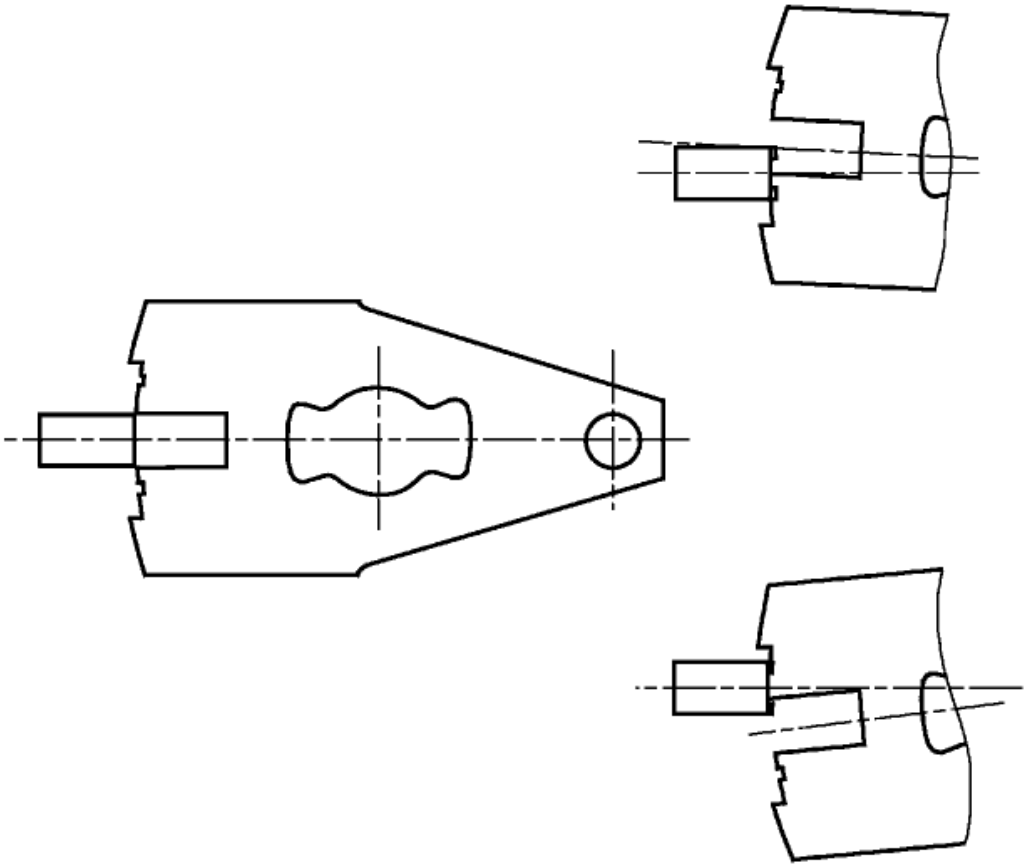


Figura B.5 – Diagrama esquemático demostrativo de ranuras falsas

B.2.5 Requisitos de diseño adicionales

B.2.5.1 El número mínimo de gorjas de doble acción debe ser siete (7) para las cerraduras de clase A y nueve (9) para las cerraduras de clase B. Las gorjas de doble acción son aquellas que tienen que ser levantadas a una determinada altura para alinear sus ranuras de entrada con la posición del pasador. En el caso de elevarse más de lo debido o menos, esta diferencia de alineación, de las ranuras de las gorjas, impedirá el movimiento del pasador a través de ellas para retirar el pestillo.

B.2.5.2 El área de la sección transversal del orificio de la cerradura no debe ser superior a 100 mm^2.

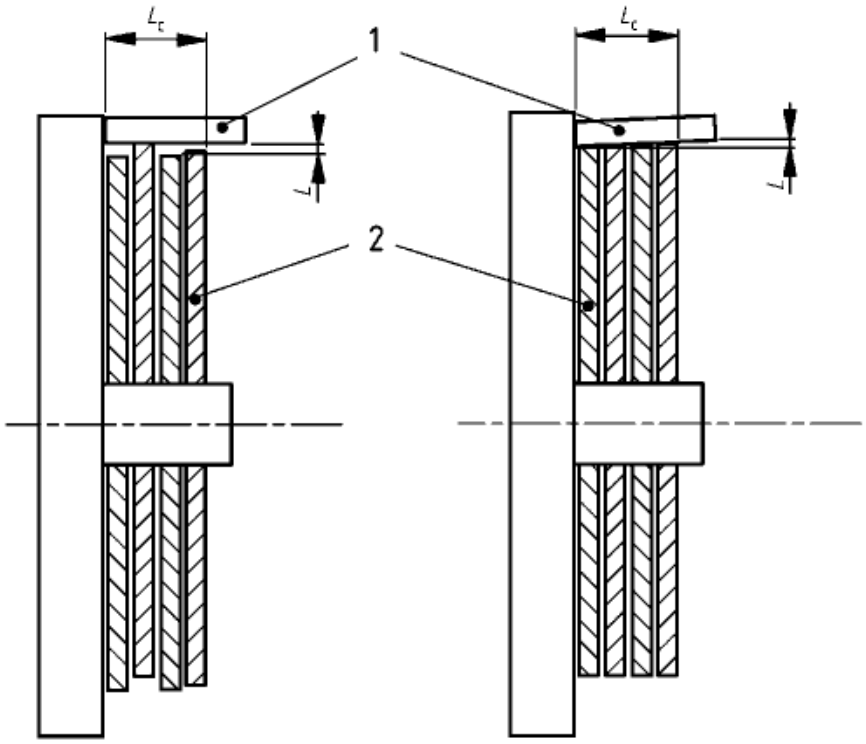
B.2.5.3 No debe ser posible obtener detalles sobre el código de apertura por la forma de las gorjas o por el número de ellas con el cual se pueden levantar las gorjas. Si no se cumple este requisito, se debería llevar a cabo un ensayo de manipulación para establecer si se cumplen los requisitos de las clases A y B.

B.3 Cerraduras de combinación mecánica

B.3.1 Generalidades

El mecanismo de identificación de código de las CAS mecánicas de combinación del tipo utilizado en este ejemplo supone la introducción de un elemento de guarda en las ranuras de los discos cuando todos los discos están correctamente alineados. Para dichas cerraduras, la resistencia a la manipulación depende de cierta tolerancia en las dimensiones y de las características de diseño de los discos, ranuras de los discos y la guarda.

Las cerraduras de combinación de las CAS de clase A y clase B que cumplan con los criterios de los apartados B.2.2 y B.2.3 se consideran suficientemente resistentes a la manipulación (véase la tabla 1) y no deben requerir ensayo de manipulación (véase 8.2.2).



Leyenda
1 Guarda
2 Discos

Figura B.6 – Diagrama esquemático que ilustra la separación entre guarda y discos

B.3.2 Guarda

Se mide la fuerza con la que la guarda entra en contacto con el conjunto de discos. Si la fuerza no es superior a 0,35 N, entonces la distancia entre la guarda y cualquier disco debe satisfacer la siguiente expresión:

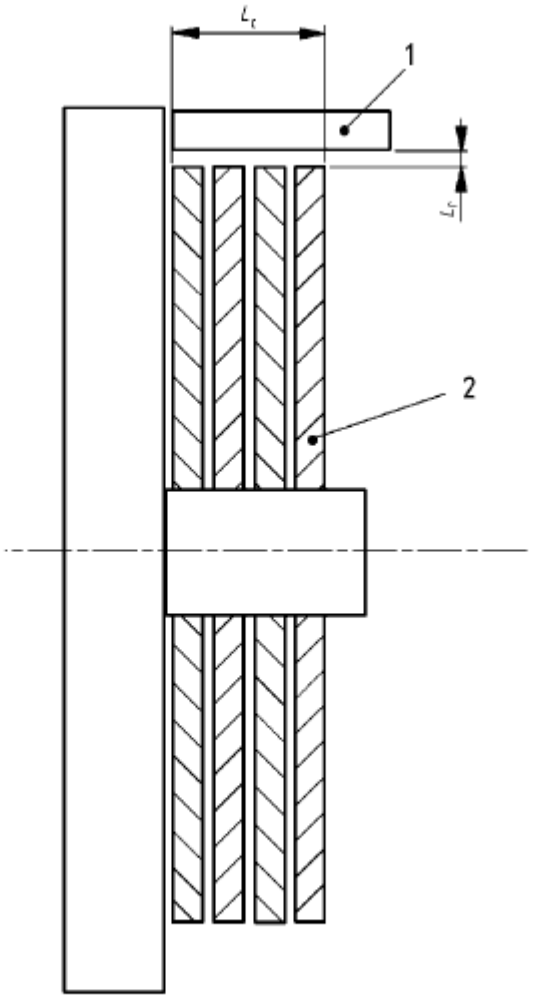
$$L \leq \frac{L_c}{50}$$

donde

L es la distancia entre el frente de la guarda de entrada y la superficie de cualquier disco (siendo esas partes del disco cualquiera menos la ranura que podría entrar en contacto con el frente de la guarda de entrada en caso de no impedirlo los otros discos), véase la figura B.6;

L_c es la anchura del conjunto de discos.

Cuando la fuerza con la que la guarda contacta con el conjunto de discos supera los 0,35 N el valor de L para cualquiera de los discos no debe superar los 0,2 mm.



Leyenda
1 Guarda levantada
2 Discos

Figura B.7 – Guarda levantada y separada de los discos

B.2.3 Ensayo de desgaste

Después del ensayo cíclico de fiabilidad (véase 8.3.1) y con la guarda levantada, la distancia (L_r) entre el frente de la guarda de entrada y la superficie de los discos (véase la figura B.7), debe satisfacer la siguiente expresión:

$$L_r \geq \frac{L_c}{100}$$

Anexo C (Normativo)

Declaración del fabricante (aplicable solo a cerraduras accionadas con llave)

Declaramos que durante la fabricación de la siguiente cerradura (CAS) accionada con llave: Modelo _____ en nuestra fábrica _____, se tomaron las siguientes medidas:

Variaciones del código:

Se ha creado una tabla de combinaciones que permite el siguiente número de códigos utilizables: _____.

Se garantiza que un código no se podrá repetir hasta haberse utilizado, por lo menos, otros _____ códigos diferentes.

Requisitos

Se han observado las siguientes restricciones durante la selección de códigos:

a. No se ha utilizado ningún precedente fijo ni esquema previamente existente para su cálculo.

b. No se han utilizado, en la cerradura, más del 40% de cortes/alturas de alzada en el código iguales, sobre el total de gorjas existentes (1).

c. No se han colocado, en la cerradura, más de dos cortes/alturas de alzada en el código iguales de forma contigua (1).

d. La diferencia entre los cortes/alturas, más altos y más bajos, de alzada en el código, es superior al 60% de la diferencia máxima de alturas de la cerradura.

Marcado de la llave

a. En la llave no hay letras, números o símbolos, con los que pudiera ser identificado el código de apertura.

b. Ninguna documentación (cualquiera que sea el formato), que pueda acompañar a la llave, proporciona información sobre el código.

Conocimiento de la ubicación de la llave

Se han implementado las medidas necesarias para evitar que las personas directamente involucradas, en la fabricación de las cerraduras, puedan tener conocimiento del domicilio de los clientes a las que les son enviadas.

Sistemas distribuidos

Si las claves criptográficas no fuesen modificables in situ (solo en las CAS de clase A), se implementan medidas que impidan que las personas directamente involucradas en la fabricación de las cerraduras, puedan tener conocimiento del domicilio de los clientes a las que les son enviadas.

Firma: _____
Nombre (impreso): _____
Fecha: _____
Cargo en la empresa: _____

(1) En el caso de cerraduras con códigos variables, la declaración se refiere a la llave.

Anexo D (Informativo)

Dimensiones de las cerraduras

Medidas en milímetros

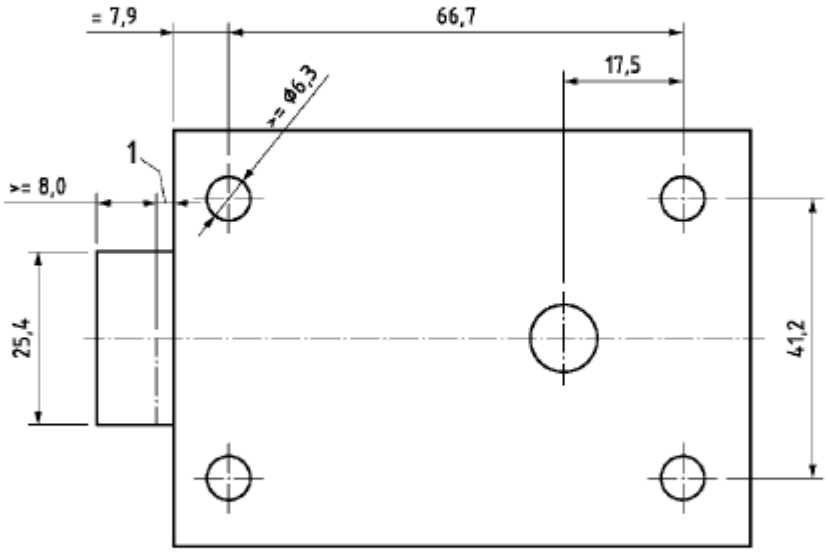


Figura D.1 – Dimensiones de la cerradura

Los salientes del pestillo ≤ 1 mm cuando la cerradura está abierta.

Anexo E (Informativo)

A – Desviaciones

Esta norma europea no resulta afectada por ninguna Directiva de la UE.

En los países del CEN/CENELEC relevantes estas A-Desviaciones son válidas en lugar de lo previsto por la norma europea hasta que hayan sido suprimidas.

Requisitos adicionales para Suecia:

Referencias a leyes y reglamentos nacionales suecos existentes relativos a la utilización de cerraduras de alta seguridad.

La Norma EN 1300:2013 no cumple los requisitos de la legislación y de los reglamentos nacionales suecos (véase la tabla 1).

La Norma EN 1300:2013 no responde a los requisitos legales suecos siguientes:

- El apartado 5.1.5.3 de la Norma EN 1300:2013 no es compatible con los reglamentos suecos: la ley sueca no reconoce las CAS controladas remotamente como sistemas distribuidos.
- Resistencia a la manipulación, mínimo M 180.
- Ensayo de temperatura: -40 °C/30 min y +70 °C/16 h.
- Ensayo cíclico. 25 000 ciclos. 25 000 ciclos correspondientes a entorno 15 años de uso diario (5 aperturas/cierres al día). Tras el ensayo cíclico, la cerradura debe someterse a ensayo con una llave que tenga media muesca de error en su posición más alta. Debe ser imposible abrir la cerradura con este ensayo.
- Compatibilidad electromagnética (EMC) – Parte 4-4: Técnicas y ensayos de medida. Ensayos de inmunidad a los transitorios eléctricos rápidos en ráfagas. EN 61000-4-37.

Tabla E.1

Documento	Referencia	Emitido por	Comentario
Vapenlagen – Ley sobre armas	SFS 1996:67	Ley nacional sueca – Parlamento sueco	**Ley sueca sobra armas (SFS 1996:67)** En el marco de la ley sobre armas, se estipula que cualquier persona que posea armas de fuego o municiones está obligado a garantizar que ninguna persona no autorizada pueda acceder a ellas. Por consiguiente, todas las armas de fuego, incluidas sus partes esenciales y las municiones, deben almacenarse en armarios de seguridad, en cajas fuertes o en cámaras acorazadas ensayadas y certificadas de acuerdo a la NORMA SOBRE ARMARIOS DE SEGURIDAD. Las reglas anteriores también estipulan que antes de abandonar los locales en los que se almacenan las armas y la munición, debe asegurarse que el armario de seguridad se ha cerrado con pestillo de acuerdo al menos a la clase B de la NORMA SOBRE LAS CERRADURAS DE ALTA SEGURIDAD. Además, las autoridades policiales suecas tienen el derecho de verificar si las armas se almacenan de la manera correcta. Un almacenamiento inadecuado puede ocasionar la revocación de la licencia de armas de fuego.
Ley sobre el acceso público a la información y secreto	SFS 1967:1997	Ley nacional sueca – Parlamento sueco	
Reglamentos y recomendaciones generales relativas a la ley sobre armas	FAP 551-3	Dirección nacional de la policía	
Reglamentos y recomendaciones generales sobre el almacenamiento y el transporte de armas de fuego y municiones por parte de la policía y otras autoridades públicas.	FAP 943-1	Dirección nacional de la policía	
Reglamentos y recomendaciones generales sobre el almacenamiento de armas de fuego por parte de los comerciantes de armas de fuego y las asociaciones	FAP 556-2	Dirección nacional de la policía	

Documento	Referencia	Emitido por	Comentario
Reglamentos y recomendaciones generales en materia de protección de la seguridad	FAP 244-1	Dirección nacional de la policía	
Almacenamiento de explosivos	SRVFS 2006:10	MSB – Agencia sueca de protección civil	

Bibliografía

[1] EN 60721-3-3, *Classification of environmental conditions. Part 3: Classification of groups of environmental parameters and their severities. Section 3: Stationary use at weatherprotected locations. (IEC 60721-3-3).*

[2] EN 60721-3-4, *Classification of environmental conditions. Part 3: Classification of groups of environmental parameters and their severities. Section 4: Stationary use at non-weatherprotected locations. (IEC 60721-3-4).*

[3] EN ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories. (ISO/IEC 17025).*

[4] NIST SP 800-57, *Recommendation for Key Management. Part 1: General.*

[5] NIST SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher.*

[6] FIPS PUB 140-2, *Security Requirements for Cryptographic Modules.*

[7] FIPS 197, *Advanced Encryption Standard (AES).*