

Requisitos de seguridad comunes para equipos radioeléctricos

Parte 3: Equipos radioeléctricos conectados a Internet que procesan dinero virtual o valor monetario

Esta norma ha sido elaborada por el comité técnico CTN-UNE 320 *Ciberseguridad y protección de datos*, cuya secretaría desempeña UNE.

EXTRACTO DEL DOCUMENTO UNE-EN 18031-3

UNE-EN 18031-3

Requisitos de seguridad comunes para equipos radioeléctricos

Parte 3: Equipos radioeléctricos conectados a Internet que procesan dinero virtual o valor monetario

Common security requirements for radio equipment. Part 3: Internet connected radio equipment processing virtual money or monetary value.

Exigences de sécurité communes applicables aux équipements radioélectriques. Partie 3: Équipements radioélectriques connectés à l'internet qui traitent une monnaie virtuelle ou de la valeur monétaire.

Esta norma es la versión oficial, en español, de la Norma Europea EN 18031-3:2024.

EXTRACTO DEL DOCUMENTO UNE-EN 18031-3

Las observaciones a este documento han de dirigirse a:

Asociación Española de Normalización

Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org

© UNE 2025

Prohibida la reproducción sin el consentimiento de UNE.

Todos los derechos de propiedad intelectual de la presente norma son titularidad de UNE.

Índice

Prólogo europeo	7
0 Introducción.....	8
1 Objeto y campo de aplicación.....	8
2 Normas para consulta	8
3 Términos y definiciones.....	8
4 Abreviaturas.....	13
5 Aplicación de este documento	14
6 Requisitos.....	17
6.1 [ACM] Mecanismo de control de acceso	17
6.1.1 [ACM-1] Aplicabilidad de los mecanismos de control de acceso.....	17
6.1.2 [ACM-2] Mecanismos de control de acceso adecuados	23
6.2 [AUM] Mecanismo de autenticación	28
6.2.1 [AUM-1] Aplicabilidad de los mecanismos de autenticación.....	28
6.2.2 [AUM-2] Mecanismos de autenticación adecuados	41
6.2.3 [AUM-3] Validación de autenticador	48
6.2.4 [AUM-4] Cambio de autenticadores	52
6.2.5 [AUM-5] Fuerza de la contraseña.....	56
6.2.6 [AUM-6] Protección contra ataques de fuerza bruta	64
6.3 [SUM] Mecanismo de actualización segura	68
6.3.1 [SUM-1] Aplicabilidad de los mecanismos de actualización.....	68
6.3.2 [SUM-2] Actualizaciones seguras.....	72
6.3.3 [SUM-3] Actualizaciones automáticas.....	77
6.4 [SSM] Mecanismo de almacenamiento seguro.....	81
6.4.1 [SSM-1] Aplicabilidad de los mecanismos de almacenamiento seguro	81
6.4.2 [SSM-2] Protección adecuada de la integridad para mecanismos de almacenamiento seguro.....	86
6.4.3 [SSM-3] Protección adecuada de la confidencialidad para mecanismos de almacenamiento seguro	91
6.5 [SCM] Mecanismo de comunicación segura	97
6.5.1 [SCM-1] Aplicabilidad de los mecanismos de comunicación segura.....	97
6.5.2 [SCM-2] Protección adecuada de la integridad y de la autenticidad para mecanismos de comunicación segura	102
6.5.3 [SCM-3] Protección adecuada de la confidencialidad para mecanismos de comunicación segura.....	108
6.5.4 [SCM-4] Protección adecuada contra ataques de repetición para mecanismos de comunicación segura.....	114
6.6 [LGM] Mecanismo de registro	120
6.6.1 [LGM-1] Aplicabilidad de los mecanismos de registro	120
6.6.2 [LGM-2] Almacenamiento persistente de datos de registro	123
6.6.3 [LGM-3] Número mínimo de eventos almacenados de manera permanente	126
6.6.4 [LGM-4] Información relacionada con el tiempo de los datos de registro almacenados de manera permanente.....	129
6.7 [CCK] Clave criptográfica confidencial	133
6.7.1 [CCK-1] Claves criptográficas confidenciales (CCK) adecuadas	133
6.7.2 [CCK-2] Mecanismos de generación de CCK.....	138

6.7.3	[CCK-3] Prevención de valores predeterminados estáticos para CCK preinstalados	142
6.8	[GEC] Capacidades generales del equipo	146
6.8.1	[GEC-1] <i>Software</i> y <i>hardware</i> actualizados sin vulnerabilidades explotables públicamente conocidas	146
6.8.2	[GEC-2] Limitar la exposición de servicios a través de interfaces de red relacionadas	152
6.8.3	[GEC-3] Configuración de servicios opcionales y las interfaces de red expuestas relacionadas	156
6.8.4	[GEC-4] Documentación de interfaces de red expuestas y servicios expuestos a través de interfaces de red	160
6.8.5	[GEC-5] Sin interfaces externas innecesarias.....	163
6.8.6	[GEC-6] Validación de entradas.....	166
6.8.7	[GEC-7].....	171
6.8.8	[GEC-8] Integridad del equipo	171
6.9	[CRY] Criptografía	175
6.9.1	[CRY-1] Mejores prácticas criptográficas	175
Anexo A (Informativo) Justificación		181
A.1	Generalidades.....	181
A.2	Justificación	181
A.2.1	Familia de normas.....	181
A.2.2	Seguridad desde el diseño.....	181
A.2.3	Modelado de amenazas y evaluación de riesgos de seguridad	182
A.2.4	Evaluación de la suficiencia funcional	183
A.2.5	Categorías de implementación	184
A.2.6	Activos	184
A.2.7	Mecanismos	186
A.2.8	Criterios de evaluación.....	187
A.2.9	Interfaces.....	190
Anexo B (Informativo) Correspondencia con la Norma EN IEC 62443-4-2:2019.....		193
B.1	Generalidades.....	193
B.2	Correspondencia.....	193
Anexo C (Informativo) Correspondencia con la Norma ETSI EN 303 645 (Ciberseguridad para el Internet de las Cosas de Consumo: Requisitos Básicos)		195
C.1	Generalidades.....	195
C.2	Correspondencia.....	195
Anexo D (Informativo) Correspondencia con la Norma de Evaluación de Seguridad para Plataformas IoT (SESIP).....		199
D.1	Generalidades.....	199
D.2	Correspondencia.....	199
Anexo ZA (Informativo) Relación entre esta norma europea y el Reglamento Delegado (UE) 2022/30 que completa la Directiva 2014/53/UE del Parlamento Europeo y del Consejo en lo que respecta a la aplicación de los requisitos esenciales contemplados en el artículo 3, capítulo 3, letras d), e) y f), de dicha Directiva		201
Bibliografía		202

Prólogo europeo

Esta Norma EN 18031-3:2024 ha sido elaborada por el Comité Técnico CEN/CENELEC JTC 13 *Ciberseguridad y protección de datos*, cuya Secretaría desempeña DIN.

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 febrero de 2025, y todas las normas nacionales técnicamente divergentes deben anularse antes de finales de febrero de 2025.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento estén sujetos a derechos de patente. CEN no es responsable de la identificación de dichos derechos de patente.

Esta norma europea ha sido elaborada bajo una solicitud de normalización dirigida a CEN por la Comisión Europea. El Comité Permanente de los Estados de la Asociación Europea de Libre Comercio aprueba en consecuencia estas solicitudes para sus Estados miembros.

La relación con la legislación de la UE se recoge en el anexo informativo ZA, que forma parte integrante de esta norma.

Cualquier comentario o pregunta sobre este documento deberían dirigirse al organismo nacional de normalización del usuario. En la web de CEN se puede encontrar un listado completo de estos organismos.

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, 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, República de Macedonia del Norte, Rumanía, Serbia, Suecia, Suiza y Turquía.

0 Introducción

Se requiere vigilancia por parte de los fabricantes para mejorar la resiliencia general contra las amenazas de ciberseguridad causadas por la mayor conectividad de los equipos radioeléctricos [34] y la creciente capacidad de los actores maliciosos para causar daño a los usuarios, las organizaciones y la sociedad.

Los requisitos de seguridad presentados en esta norma básica se desarrollan para mejorar la capacidad de los equipos radioeléctricos para proteger sus activos de seguridad y financieros contra amenazas comunes de ciberseguridad y mitigar vulnerabilidades explotables públicamente conocidas.

Es importante destacar que, para lograr la ciberseguridad integral de los equipos radioeléctricos, será necesario que tanto el fabricante como el usuario apliquen las mejores prácticas de defensa en profundidad. En particular, ninguna medida única será suficiente para lograr los objetivos dados; de hecho, lograr incluso un solo objetivo de seguridad generalmente requerirá un conjunto de mecanismos y medidas. A lo largo de este documento, el material de orientación incluye listas de ejemplos. Estos ejemplos indicados son solo posibilidades indicativas, ya que existen otras posibilidades que no se enumeran, e incluso usar los ejemplos indicados no será suficiente a menos que los mecanismos y medidas elegidos se implementen de manera coordinada.

1 Objeto y campo de aplicación

Este documento especifica los requisitos comunes de seguridad y los criterios de evaluación relacionados para los equipos radioeléctricos conectados a Internet [35]. Dichos equipos permiten al titular o usuario transferir dinero, valor monetario o moneda virtual [35] (en adelante, “equipos”).

2 Normas para consulta

No hay normas para consulta en este documento.