Norma Española

UNE-EN 18031-3

Marzo 2025

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

Asociación Española de Normalización

Calle de Génova, 6
28004 Madrid. España

915 294 900
info@une.org – www.une.org

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

Índice

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.