SOLIDWARETOOLS

CRACheck

DOCUMENTO 2

Documentación Técnica

Art. 31 + Anexo VII

NovaBridge Technologies Inc.

NovaBridge SmartHub v3.1

Referencia: CRACHK-NYCRWG
Fecha de emisión: 15/10/2026
Contacto: Sarah Chen, VP of Compliance
compliance@novabridge.io

Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo
de 23 de octubre de 2024 (Cyber Resilience Act)

Este documento no constituye asesoramiento jurídico. Responsabilidad exclusiva del fabricante.

1 DESCRIPCIÓN GENERAL DEL PRODUCTO (Anexo VII, punto 1)

PROPÓSITO PREVISTO [Anexo VII, 1(a)]

Hub domótico WiFi/Zigbee para control centralizado de dispositivos smart home (luces, cerraduras inteligentes, cámaras de seguridad, sensores de movimiento y temperatura). Incluye app móvil iOS/Android y backend cloud (AWS eu-west-1) para acceso remoto y notificaciones push. Destinado a consumidores residenciales en la UE, vendido a través de Amazon.de, Amazon.fr y Amazon.es.

VERSIÓN SOFTWARE [Anexo VII, 1(b)]

3.1.0

TIPO DE PRODUCTO

Hardware + software (dispositivo IoT, electrodoméstico conectado, etc.)

TRATAMIENTO DE DATOS A DISTANCIA

Sí — El producto depende de un servicio cloud/backend del fabricante

DETALLE

Backend cloud en AWS (eu-west-1) para: acceso remoto al hub vía app móvil, almacenamiento de configuraciones y escenas, distribución de actualizaciones OTA, notificaciones push de eventos de seguridad. Sin este backend, el control remoto y las notificaciones no funcionan (el control local vía Zigbee sí funciona).

INFORMACIÓN AL USUARIO [Anexo VII, 1(d)]

Ver Documento 4 — Información e Instrucciones al Usuario

Este documento no constituye asesoramiento jurídico. Responsabilidad exclusiva del fabricante.

2 DISEÑO, DESARROLLO, PRODUCCIÓN Y VULNERABILIDADES (Anexo VII, punto 2)

2(a) Diseño y desarrollo

La arquitectura del sistema y la descripción de cómo los componentes software se integran se detallan en la evaluación de riesgos (Documento 3) y en las respuestas a los requisitos esenciales del Anexo I.

2(b) Gestión de vulnerabilidades

SBOM [Anexo VII, 2(b)]

Sí — SBOM generado y mantenido — Formato: CycloneDX — Dependencias de nivel superior: 47

POLÍTICA CVD [Anexo VII, 2(b)]

Política de divulgación coordinada publicada en https://www.novabridge.io/security/cvd-policy. Canal de reporte: security@novabridge.io + formulario web HTTPS. Compromiso de acuse de recibo en 48 horas laborables. Tiempo de remediación objetivo: 90 días desde la confirmación de la vulnerabilidad. Divulgación pública coordinada tras la disponibilidad del parche. Programa de bug bounty activo en HackerOne (https://hackerone.com/novabridge) con recompensas de $100-$5,000 según severidad CVSS.

CONTACTO DE VULNERABILIDADES [Art. 13.17]

security@novabridge.io · https://www.novabridge.io/security · +1 302 555 0142 (horario EST)

DISTRIBUCIÓN SEGURA DE UPDATES [Anexo VII, 2(b)]

OTA (Over-The-Air) con firma digital de paquetes Ed25519. Canal cifrado TLS 1.3 punto a punto. Verificación de integridad del firmware (SHA-256) antes y después de la instalación. Rollback automático al firmware anterior en caso de fallo de verificación. Actualizaciones de seguridad separadas de las funcionales siempre que es técnicamente viable. Cada actualización de seguridad permanece disponible para descarga durante un mínimo de 10 años (Art. 13.9).

2(c) Producción y monitorización

Los procesos de producción, control de calidad y monitorización continua son responsabilidad del fabricante. Las medidas de verificación incluyen los tests de seguridad documentados en el punto 6 de esta documentación técnica.

Este documento no constituye asesoramiento jurídico. Responsabilidad exclusiva del fabricante.

3 EVALUACIÓN DE RIESGOS DE CIBERSEGURIDAD (Anexo VII, punto 3)

La evaluación completa de riesgos conforme al Art. 13.2-4, incluyendo el mapeo contra los requisitos esenciales del Anexo I, se encuentra en el Documento 3 (Evaluación de Riesgos de Ciberseguridad) de este dossier.

4 PERIODO DE SOPORTE (Anexo VII, punto 4)

PERIODO DE SOPORTE [Art. 13.8]

5 años — hasta 03/2031

JUSTIFICACIÓN [Anexo VII, punto 4]

Periodo de 5 años basado en: (1) vida útil esperada de un hub domótico según estudios de mercado (Consumer Technology Association: 5-7 años para dispositivos smart home); (2) coherencia con periodos de soporte de productos similares en el mercado (Google Nest Hub: 5 años, Amazon Echo: 4 años, Samsung SmartThings: 5 años); (3) disponibilidad del entorno operativo (Android/iOS soportan dispositivos durante ~5 años); (4) periodos de soporte de productos comparables en el mercado.

5 ESTÁNDARES Y ESPECIFICACIONES APLICADOS (Anexo VII, punto 5)

ESTÁNDARES APLICADOS [Art. 27]

ETSI EN 303 645 v2.1.1 (2020-06): Cyber Security for Consumer Internet of Things — aplicado en su totalidad. ISO/IEC 27001:2022: Sistema de gestión de seguridad de la información — certificación en curso (auditoría en curso). IEC 62443-4-1:2018: Secure product development lifecycle — aplicado al proceso de desarrollo. NIST SP 800-183: Networks of Things — utilizado como referencia para la arquitectura de seguridad IoT. No hay estándares armonizados CRA (Reg. 2024/2847) publicados en el DOUE a la fecha de emisión de este dossier.

6 INFORMES DE TEST (Anexo VII, punto 6)

RESUMEN DE TESTS REALIZADOS [Anexo VII, punto 6]

(1) Penetration test externo — NCC Group, informe ref: NCG-2026-0412, fecha: 15/03/2026. Resultado: 0 vulnerabilidades críticas, 1 media (corregida en v3.1.0-patch2), 3 informativas. (2) Análisis estático de código — SonarQube v10.4, última ejecución: 01/04/2026. Resultado: 0 bugs críticos, 0 vulnerabilidades, 2 code smells menores. (3) Escaneo de dependencias — Snyk, última auditoría: 20/04/2026. Resultado: 0 CVE conocidos en dependencias directas, 47 dependencias totales escaneadas. (4) Fuzzing de protocolo MQTT — AFL++ v4.09c, 72h de ejecución. Resultado: 0 crashes reproducibles.

7 DECLARACIÓN UE DE CONFORMIDAD (Anexo VII, punto 7)

Ver Documento 5 de este dossier — Declaración UE de Conformidad conforme al Art. 28 y Anexo V.

8 SBOM — SOFTWARE BILL OF MATERIALS (Anexo VII, punto 8)

El fabricante mantiene el SBOM en formato CycloneDX, con 47 dependencias de nivel superior. Se proporciona bajo solicitud razonada de la autoridad de vigilancia del mercado, conforme al Anexo VII, punto 8.

Este documento ha sido generado por CRACheck (SolidwareTools) a partir de la información facilitada por el fabricante. No constituye asesoramiento jurídico ni una auditoría de terceros. La veracidad de los datos y el cumplimiento efectivo de las obligaciones legales aplicables son responsabilidad exclusiva del fabricante. La estructura sigue el Reglamento (UE) 2024/2847 según la revisión de SolidwareTools a la fecha de emisión. Para asesoramiento personalizado, consulte con un profesional cualificado.