SOLIDWARETOOLS

CRACheck

DOCUMENTO 4

Información e Instrucciones al Usuario

Anexo II

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.

>> INFORMACIÓN OBLIGATORIA (Anexo II)

1. Datos del fabricante

NOMBRE [Anexo II, punto 1]
NovaBridge Technologies Inc.

DIRECCIÓN
1200 Tech Park Drive, Suite 400, Wilmington, DE 19801, USA

EMAIL
compliance@novabridge.io

WEB
https://www.novabridge.io

2. Punto de contacto de vulnerabilidades

CONTACTO [Anexo II, punto 2]
security@novabridge.io · https://www.novabridge.io/security · +1 302 555 0142 (horario EST)

POLÍTICA CVD
Disponible en el sitio web del fabricante

3. Identificación del producto

NOMBRE Y TIPO [Anexo II, punto 3]
NovaBridge SmartHub v3.1

VERSIÓN
3.1.0

TIPO/LOTE/SERIE
SH-2026-LOT04

4. Propósito previsto y entorno de seguridad

PROPÓSITO PREVISTO [Anexo II, punto 4]
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.

5. Riesgos conocidos de ciberseguridad

CIRCUNSTANCIAS DE RIESGO [Anexo II, punto 5]
(1) Uso en redes WiFi abiertas o con cifrado débil (WEP) puede exponer la comunicación entre el hub y el router. Mitigación: el hub rechaza conexiones a redes sin WPA2/WPA3. (2) No actualizar el firmware puede dejar el dispositivo vulnerable a exploits conocidos. Mitigación: actualizaciones automáticas activadas por defecto. (3) Reutilización del dispositivo sin factory reset puede exponer datos y configuraciones del usuario anterior. Mitigación: advertencia visible en la app al desvincular el dispositivo. (4) Contraseñas débiles de la cuenta cloud pueden permitir acceso no autorizado al control remoto. Mitigación: requisitos de complejidad de contraseña + MFA recomendado en el primer uso.

6. Declaración de conformidad

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

ACCESO [Anexo II, punto 6]

Ver Documento 5 de este dossier o en la web del fabricante

7. Soporte técnico y periodo de soporte

PERIODO DE SOPORTE [Anexo II, punto 7]

5 años — hasta 03/2031

TIPO DE SOPORTE

Actualizaciones de seguridad gratuitas durante todo el periodo de soporte

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

8. Instrucciones detalladas

8(A) INSTALACIÓN Y USO SEGURO [Anexo II, 8(a)]

1. Conectar únicamente a red WiFi protegida con WPA2 o WPA3. 2. Cambiar la contraseña de administrador durante la configuración inicial (el sistema lo exige). 3. Activar la autenticación en dos factores (MFA) en la app móvil NovaBridge. 4. Mantener el firmware actualizado — las actualizaciones automáticas están activadas por defecto. 5. No exponer el puerto de gestión local (443) a internet; usar siempre la conexión cloud segura para acceso remoto. 6. Revisar periódicamente los dispositivos Zigbee pareados y eliminar los desconocidos. 7. Revisar los logs de acceso en la app (Ajustes > Seguridad > Historial de accesos).

8(B) CAMBIOS Y SEGURIDAD DE DATOS [Anexo II, 8(b)]

Las actualizaciones de firmware pueden modificar configuraciones de seguridad. Se recomienda revisar la configuración tras cada actualización mayor.

8(C) INSTALACIÓN DE ACTUALIZACIONES [Anexo II, 8(c)]

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).

8(D) DESCOMISIONADO SEGURO [Anexo II, 8(d)]

Factory reset desde la app (Ajustes > Sistema > Restaurar valores de fábrica) o botón físico en el dispositivo (mantener 5 segundos). El reset borra: todas las credenciales WiFi almacenadas, tokens de acceso cloud, configuraciones y escenas, lista de dispositivos Zigbee pareados, logs de eventos locales. Tras el reset, el hub se desvincula automáticamente de la cuenta cloud del usuario. El usuario puede solicitar la eliminación completa de sus datos del cloud en https://www.novabridge.io/privacy/data-deletion.

8(E) DESACTIVAR ACTUALIZACIONES AUTOMÁTICAS [Anexo II, 8(e)]

[A completar por el fabricante: cómo puede el usuario desactivar la instalación automática de actualizaciones de seguridad, cuando proceda]

9. SBOM

DISPONIBILIDAD DEL SBOM [Anexo II, punto 9]

El fabricante pone a disposición del usuario el SBOM bajo solicitud. Contactar a security@novabridge.io · https://www.novabridge.io/security · +1 302 555 0142 (horario EST)

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.