SOLIDWARETOOLS

CRACheck

DOCUMENTO 3

Evaluación de Riesgos de Ciberseguridad

Art. 13.2-4 + Anexo I

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.

>> CONTEXTO DE LA EVALUACIÓN

Esta evaluación de riesgos documenta el análisis realizado conforme al Art. 13.2 del Reglamento (UE) 2024/2847, tomando en cuenta el propósito previsto, el uso razonablemente previsible y las condiciones de uso del producto, con el objetivo de minimizar los riesgos de ciberseguridad, prevenir incidentes y minimizar su impacto.

PRODUCTO EVALUADO

NovaBridge SmartHub v3.1

PROPÓSITO PREVISTO

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.

ENTORNO OPERATIVO

Hogares en la UE. El hub se conecta al router WiFi doméstico y a la nube del fabricante (AWS eu-west-1) para el acceso remoto; los dispositivos Zigbee se emparejan en local. Instalado y usado por consumidores no expertos. Mal uso razonablemente previsible: red doméstica sin proteger, producto expuesto a internet por redirección de puertos hecha por el usuario.

PERIODO DE SOPORTE EVALUADO

5 años

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

>> REQUISITOS ESENCIALES — PARTE I: PROPIEDADES DEL PRODUCTO (Anexo I)

Para cada requisito del Anexo I, Parte I, se indica si aplica al producto y se describe la implementación o, en caso de no aplicar, la justificación conforme al Art. 13.4.

(a) Sin vulnerabilidades explotables conocidas

APLICA

IMPLEMENTACIÓN [Anexo I, Parte I, 2(a)]

Escaneo CVE completo de todas las dependencias (Snyk) y test de penetración (NCC Group, informe NCG-2026-0412) completados el 15/03/2026. 0 vulnerabilidades críticas o altas pendientes al momento de lanzamiento. Proceso de verificación pre-release documentado en el QMS.

(b) Configuración segura por defecto

APLICA

IMPLEMENTACIÓN [Anexo I, Parte I, 2(b)]

Configuración de fábrica: WiFi desactivado hasta configuración inicial, credenciales de administrador únicas por dispositivo (generadas en fábrica con CSPRNG), Zigbee pairing mode desactivado por defecto. Factory reset disponible: botón físico (5 segundos) + opción en app + opción en interfaz web local.

(c) Actualizaciones de seguridad

APLICA

IMPLEMENTACIÓN [Anexo I, Parte I, 2(c)]

Actualizaciones OTA automáticas activadas por defecto. El usuario puede desactivarlas desde Ajustes > Sistema > Actualizaciones automáticas. Notificación push cuando hay actualización disponible. Actualizaciones de seguridad separadas de las funcionales cuando es técnicamente viable. Opción de postponer actualización hasta 7 días.

(d) Protección contra acceso no autorizado

APLICA

IMPLEMENTACIÓN [Anexo I, Parte I, 2(d)]

Autenticación por email/contraseña + MFA opcional (TOTP). Sesiones con JWT, expiración 24h. Control de acceso: admin / usuario estándar / invitado. Logging de todos los intentos de acceso (exitosos y fallidos) con IP, timestamp y user-agent. Bloqueo de cuenta tras 5 intentos fallidos (30 min).

(e) Confidencialidad de datos

APLICA

IMPLEMENTACIÓN [Anexo I, Parte I, 2(e)]

TLS 1.3 para toda comunicación hub-cloud y app-cloud. AES-256-GCM para datos sensibles en reposo (credenciales WiFi, tokens). Certificados X.509 con pinning en la app móvil. Zigbee con cifrado AES-128-CCM (estándar Zigbee 3.0).

(f) Integridad de datos

APLICA

IMPLEMENTACIÓN [Anexo I, Parte I, 2(f)]

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

Secure boot con verificación de firma Ed25519 del firmware en cada arranque. Verificación de integridad de configuración mediante HMAC-SHA256. Firma digital de todos los paquetes de actualización OTA. Reporte automático al usuario si se detecta modificación no autorizada de la configuración.

(g) Minimización de datos

APLICA

IMPLEMENTACIÓN [Anexo I, Parte I, 2(g)]

Datos recogidos: configuración de dispositivos, escenas programadas, logs de eventos (últimos 30 días), token de autenticación cloud. No se recogen datos de uso del hogar, grabaciones de audio/vídeo (las cámaras se procesan localmente), ni geolocalización precisa. Política de retención: logs eliminados automáticamente a los 30 días.

(h) Disponibilidad y resiliencia

APLICA

IMPLEMENTACIÓN [Anexo I, Parte I, 2(h)]

Modo offline: el hub funciona como controlador local Zigbee sin conexión a internet. Rate limiting en la API cloud: 100 req/min por usuario. Recuperación automática tras corte de energía (estado persistente en flash). Watchdog timer para reinicio automático en caso de cuelgue del firmware.

(i) Minimizar impacto en otros dispositivos

APLICA

IMPLEMENTACIÓN [Anexo I, Parte I, 2(i)]

Aislamiento de red: el hub no actúa como router ni reenvía tráfico entre dispositivos Zigbee e internet. Control de tráfico saliente limitado a los endpoints cloud de NovaBridge (lista blanca de dominios). Sin UPnP, sin apertura automática de puertos.

(j) Minimizar superficie de ataque

APLICA

IMPLEMENTACIÓN [Anexo I, Parte I, 2(j)]

Solo 3 puertos abiertos: 443 (HTTPS para interfaz web local), 8883 (MQTT sobre TLS para comunicación cloud), puerto Zigbee (radio, no IP). Servicios SSH y Telnet deshabilitados en producción. Interfaz de debug desactivada en firmware de producción. Principio de mínimo privilegio: cada proceso del firmware corre con los permisos mínimos necesarios.

(k) Mitigación de impacto de incidentes

APLICA

IMPLEMENTACIÓN [Anexo I, Parte I, 2(k)]

Procesos del firmware aislados mediante namespaces Linux. Partición de firmware read-only (squashfs). Datos de usuario en partición separada. Rollback automático a firmware anterior si la actualización falla la verificación de integridad post-instalación. Compartimentación: compromiso de un servicio no compromete el sistema completo.

(l) Registro y monitorización de seguridad

APLICA

IMPLEMENTACIÓN [Anexo I, Parte I, 2(l)]

Logs de seguridad: accesos, cambios de configuración, actualizaciones de firmware, eventos Zigbee

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

(pairing/unpairing), intentos de acceso fallidos. Almacenados localmente (últimos 30 días) y opcionalmente sincronizados al cloud (cifrados). El usuario puede desactivar la sincronización al cloud desde Ajustes > Privacidad. Logs locales no desactivables (necesarios para diagnóstico).

(m) Borrado seguro de datos

APLICA

IMPLEMENTACIÓN [Anexo I, Parte I, 2(m)]

Factory reset completo: botón físico (5 seg) o desde la app (Ajustes > Sistema > Restaurar valores de fábrica). Borra: credenciales WiFi, tokens cloud, configuraciones, escenas, logs, dispositivos Zigbee pareados. Exportación de datos: el usuario puede descargar sus datos en formato JSON desde la app antes del reset. La transferencia se realiza sobre HTTPS.

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

>> REGISTRO DE AMENAZAS Y RIESGOS (Art. 13.2-13.3)

Para cada requisito del Anexo I, Parte I: la amenaza que cubre, el riesgo valorado por el fabricante antes de las medidas descritas arriba y el riesgo residual después de ellas.

REQ.	AMENAZA QUE CUBRE	RIESGO ANTES	MEDIDAS	RIESGO RESIDUAL
(a)	Explotación de vulnerabilidades conocidas del producto o de sus componentes	Alto	Ver (a) arriba	Medio
(b)	Compromiso por configuración por defecto insegura o credenciales por defecto	Alto	Ver (b) arriba	Bajo
(c)	Vulnerabilidades abiertas por actualizaciones ausentes o fallidas	Alto	Ver (c) arriba	Bajo
(d)	Acceso no autorizado al producto, a sus funciones o a sus datos	Alto	Ver (d) arriba	Bajo
(e)	Revelación de datos almacenados, transmitidos o tratados	Alto	Ver (e) arriba	Bajo
(f)	Manipulación de datos, comandos, programas o configuración	Alto	Ver (f) arriba	Bajo
(g)	Tratamiento de más datos de los necesarios, con mayor exposición	Medio	Ver (g) arriba	Bajo
(h)	Pérdida de funciones esenciales, incluida la denegación de servicio	Medio	Ver (h) arriba	Medio
(i)	Uso del producto para dañar otros dispositivos o redes	Medio	Ver (i) arriba	Bajo
(j)	Explotación de interfaces o servicios innecesarios	Alto	Ver (j) arriba	Bajo
(k)	Propagación o agravamiento del impacto de un incidente	Medio	Ver (k) arriba	Bajo
(l)	Actividad maliciosa no detectada	Medio	Ver (l) arriba	Bajo
(m)	Datos que permanecen en el producto tras su retirada	Medio	Ver (m) arriba	Bajo

Riesgos residuales valorados como Altos: 0. Todo riesgo residual Alto debe revisarse antes de introducir el producto en el mercado. Los requisitos sin valorar deben ser valorados por el fabricante.

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

>> REQUISITOS ESENCIALES — PARTE II: GESTIÓN DE VULNERABILIDADES (Anexo I)

(1) Identificación y documentación de vulnerabilidades + SBOM

SBOM [Parte II, punto 1]

Sí — SBOM generado y mantenido — CycloneDX

(2) Remediación de vulnerabilidades

PROCESO [Parte II, punto 2]

Clasificación por CVSS v3.1. Críticas (CVSS ≥9.0): parche en 24-48h, notificación inmediata a usuarios. Altas (CVSS 7.0-8.9): parche en 7 días. Medias (CVSS 4.0-6.9): parche en 30 días. Bajas (CVSS <4.0): incluidas en el siguiente release programado. Todas las actualizaciones de seguridad son gratuitas durante el periodo de soporte. Información sobre vulnerabilidades corregidas publicada en https://www.novabridge.io/security/advisories tras la disponibilidad del parche (Anexo I, Parte II, punto 4).

(3) Tests y revisiones regulares

PROCESO [Parte II, punto 3]

Penetration testing trimestral por NCC Group (último informe: NCG-2026-0412, marzo 2026). Análisis estático de código con SonarQube en cada commit (0 blocker/critical permitidos para merge). Escaneo de vulnerabilidades de dependencias semanal con Snyk (integrado en CI/CD). Fuzzing de protocolos Zigbee y MQTT con AFL++ antes de cada release mayor. Revisión de seguridad manual del código por el equipo de seguridad antes de cada release.

(4) Divulgación de vulnerabilidades corregidas

PROCESO [Parte II, punto 4]

Información publicada en el sitio web del fabricante tras la disponibilidad del parche. Se incluye descripción, productos afectados, impacto, severidad y medidas de remediación.

(5) Política de divulgación coordinada (CVD)

POLÍTICA CVD [Parte II, punto 5]

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.

(6) Punto de contacto para vulnerabilidades

CONTACTO [Parte II, punto 6]

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

(7) Distribución segura de actualizaciones

MECANISMO [Parte II, punto 7]

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).

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

(8) Actualizaciones de seguridad gratuitas

POLÍTICA [Parte II, punto 8]

Todas las actualizaciones de seguridad se proporcionan de forma gratuita durante el periodo de soporte (5 años). Cada actualización permanece disponible para descarga durante un mínimo de 10 años conforme al Art. 13.9.

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.