wavecom

# Connecting every...things

Soluciones creativas e innovadoras en el ámbito de la ingeniería de comunicaciones.

# Política de Divulgación Coordinada de Vulnerabilidades

Septiembre de 2026

# Índice

# 1. Control del Documento

> *UE 2024/2847 (CRA) — art. 13(8): los fabricantes deben disponer de políticas y procedimientos para el tratamiento de vulnerabilidades. Debe existir un documento de política, versionado, con propietario asignado y revisado periódicamente.*

| Campo | Wavecom |
|---|---|
| Nombre de la organización | WAVECOM – Soluções Rádio, S.A. |
| Propietario del documento | Information Security Manager (ISM) |
| Equipo de seguridad | Wavecom Product Security Incident Response Team (PSIRT) — en constitución. Hasta su establecimiento formal, la función la desempeña el Information Security Manager junto con el Departamento de I+D. |
| Versión | 1.0 |
| Fecha de entrada en vigor | 8 de septiembre de 2026 |
| Ciclo de revisión | Anual, o antes ante un cambio significativo del producto o del marco CRA aplicable |
| Clasificación | Público |

# 2. Objeto

**WAVECOM** está comprometida con la seguridad de los productos con elementos digitales que introduce en el mercado. Esta **Política de Divulgación Coordinada de Vulnerabilidades (CVD)** describe cómo terceros — incluidos investigadores de seguridad, clientes y el público en general — pueden reportar posibles vulnerabilidades de seguridad en nuestros productos y sistemas, y cómo tratamos esos reportes.

Esta política está alineada con el Reglamento (UE) 2024/2847 (Cyber Resilience Act — CRA) y con la prEN 40000-1-3, que establece requisitos y recomendaciones para los fabricantes de productos con elementos digitales en materia de divulgación de vulnerabilidades potenciales.

# 3. Funciones y Responsabilidades

> *UE 2024/2847 (CRA) — art. 13(17): los fabricantes deben designar un punto de contacto único. El contacto debe ser fácilmente identificable, permitir que el usuario elija su medio de comunicación preferido y no puede limitarse a herramientas automatizadas.*

## 3.1 Equipo Interno de Seguridad

El equipo interno responsable de la gestión de la divulgación de vulnerabilidades es el Wavecom Product Security Incident Response Team (PSIRT), al que corresponde:

Recibir y acusar recibo de las vulnerabilidades reportadas.

Validar, evaluar y priorizar las vulnerabilidades en función del riesgo.

Coordinar las actividades de corrección con los equipos internos implicados.

Gestionar la comunicación a lo largo de todo el proceso de tratamiento de la vulnerabilidad.

Emitir avisos de seguridad y notificaciones de vulnerabilidad cuando proceda.

| Campo | Wavecom |
|---|---|
| Equipo o persona responsable de recibir los reportes | Information Security Manager (ISM), como punto de contacto único CRA, con supervisión de ciberseguranca@wavecom.pt. |
| ¿Existe un PSIRT formal? | Las actividades de ciberseguridad están actualmente repartidas en el equipo técnico de Wavecom. Está prevista la constitución de un PSIRT específico. |
| ¿Quién coordina la corrección? | Departamento de I+D, junto con el Product Security Owner de la línea de producto afectada. |
| ¿Quién aprueba la divulgación pública? | Consejo de Administración, a propuesta del ISM. |

## 3.2 Lo Que Pedimos a Quien Reporta Vulnerabilidades

Se espera que toda persona u organización que presente un reporte de vulnerabilidad actúe de buena fe y cumpla lo siguiente:

- No explotar la vulnerabilidad más allá de lo necesario para confirmar su existencia.
- No acceder, modificar ni exfiltrar datos más allá de lo estrictamente necesario para demostrar el problema.
- No divulgar públicamente la vulnerabilidad antes de que hayamos tenido una oportunidad razonable de investigarla y corregirla.
- Facilitar información suficiente para reproducir, evaluar y validar el problema reportado.
- No realizar ataques de denegación de servicio, ingeniería social ni phishing en el marco de las pruebas.

## 4. Alcance de la Política

> *CRA / prEN 40000-1-3 [PRE-2-RC-02]: la política de divulgación de vulnerabilidades debe especificar las opciones de comunicación segura, el alcance, la publicación, el reconocimiento y el contenido de los reportes. UE 2024/2847 (CRA) — anexo I, parte I, punto (2)(a): los productos deben introducirse en el mercado sin vulnerabilidades explotables conocidas, lo que exige un proceso de recepción de reportes.*

### 4.1 Productos y Sistemas Cubiertos

**Los siguientes sistemas, productos y servicios están incluidos en el alcance de esta política:**

| Producto / sistema | Versión / URL / detalle del alcance | ¿Incluye nube / aplicación? |
|---|---|---|
| Wavecom IoT Gateway | Gamas WR, WK y WT — todas las revisiones de hardware y versiones de firmware soportadas introducidas en el mercado de la UE, incluidas las unidades introducidas antes del 11 de septiembre de 2026 (CRA, art. 69(3)). Sistema operativo ejecutado en el hardware Wavecom IoT Gateway serie WR — WaveOS — versiones 2025 y posteriores. | Sí — gestionado a través de Wavecom IoT Manager |

| Producto / sistema | Versión / URL / detalle del alcance | ¿Incluye nube / aplicación? |
|---|---|---|
| Wavecom IoT Manager | Plataforma web centralizada, en SaaS y on-premises — todas las versiones soportadas, que incluyen:<br>Servicio de gestión y aprovisionamiento de gateways;<br>Servicio de gestión y aprovisionamiento de dispositivos;<br>Servicio de monitorización de flota;<br>Servicio de monitorización de agua. | No |
| Cloud Authentication System (CAS) | Servicio de autenticación de invitados Wi-Fi y control de accesos, en SaaS y on-premises, integrado en la plataforma Wavecom IoT Manager o autónomo. | No |
| WHERE IS® | Plataforma de localización RTLS y RFID, incluidos los componentes de software desarrollados por Wavecom, en SaaS y on-premises; el hardware de terceros queda cubierto por sus propios fabricantes. | No |

## 4.2 Lo Que No Está Cubierto (Fuera de Alcance)

Quedan fuera del alcance de esta política los elementos siguientes. Los reportes relativos a ellos no serán investigados:

- Productos, servicios o infraestructuras de terceros no pertenecientes ni operados por Wavecom.
- Ingeniería social, phishing o ataques a la seguridad física de Wavecom o de su personal.
- Ataques de denegación de servicio (DoS) o de denegación de servicio distribuida (DDoS).
- Productos o versiones de software en fin de vida y sin soporte.
- Vulnerabilidades ya conocidas por Wavecom o ya reportadas por un tercero.

## 5. Cómo Reportar una Vulnerabilidad

> *UE 2024/2847 (CRA) — art. 13(17): el punto de contacto único debe ser fácilmente identificable, permitir que el usuario elija su medio de comunicación preferido y no puede limitarse a herramientas automatizadas. prEN 40000-1-3 [PRE-2-RQ-02]: debe existir uno o más mecanismos de contacto. [RCP-1-RQ-01]: los mecanismos de contacto deben ser accesibles al público.*

### 5.1 Canales de Contacto

| Canal | ¿Obligatorio? | Detalle |
|---|---|---|
| Dirección de correo de seguridad | Obligatorio — buzón supervisado | ciberseguranca@wavecom.pt — buzón supervisado, operado por el Information Security Manager (ISM) como punto de contacto único CRA conforme al art. 13(17). Acuse de recibo en 3 a 5 días hábiles. |
| Teléfono / atención al cliente | Opcional — útil cuando ya existe una línea de soporte | El Soporte Técnico de Wavecom puede recibir reportes por los canales habituales de atención al cliente. Los equipos de soporte e ingeniería de campo tienen instrucciones de remitir de inmediato cualquier indicio de vulnerabilidad de seguridad o de explotación activa a ciberseguranca@wavecom.pt, y por teléfono cuando se sospeche explotación, sin evaluación técnica previa. |
| Clave PGP (para correo cifrado) | Recomendada cuando el correo es el canal principal — permite enviar información sensible de forma segura | Aún no publicada. Quien necesite transmitir información sensible debe solicitar las condiciones de cifrado en ciberseguranca@wavecom.pt. |

### 5.2 Qué Debe Incluir el Reporte

> *CRA / prEN 40000-1-3 [PRE-2-RC-02]: la política de divulgación de vulnerabilidades debe especificar el contenido esperado de los reportes.*

Pedimos que, siempre que sea posible, el reporte incluya como mínimo la información siguiente, lo que nos permite triar e investigar con rapidez:

- Nombre, modelo, versión y/o URL del producto afectado.
- Descripción clara de la vulnerabilidad y de su posible impacto en la seguridad.
- Instrucciones paso a paso para reproducir la vulnerabilidad, incluidas las herramientas y configuraciones utilizadas.
- Evidencias de apoyo — capturas de pantalla, capturas de red, ficheros de registro o código de prueba de concepto.
- Propuesta de gravedad o puntuación CVSS, si se dispone de ella (opcional).
- Datos de contacto para el seguimiento — también se aceptan reportes anónimos.

## 6. Tratamiento de Vulnerabilidades

> *CRA / prEN 40000-1-3 [PRE-2-RQ-03]: deben describirse las expectativas de comunicación con quien reporta. UE 2024/2847 (CRA) — anexo I, parte II, punto (2): las vulnerabilidades deben abordarse y corregirse sin demora indebida, incluida la puesta a disposición de actualizaciones de seguridad.*

### 6.1 Acuse de Recibo

> *CRA / prEN 40000-1-3 [RCP-1-RQ-02]: a cada reporte debe asignarse un número de seguimiento. [RCP-1-RQ-03]: el acuse de recibo debe enviarse dentro del plazo indicado en esta política.*

Tras la recepción de un posible reporte de vulnerabilidad, Wavecom acusa recibo en el plazo indicado a continuación. El acuse de recibo incluye un número de seguimiento único.

**WAVECOM** acusa recibo de todos los reportes de vulnerabilidad en un plazo de 3 a 5 días hábiles. El acuse de recibo incluye un número de seguimiento único, que debe citarse en toda correspondencia posterior.

### 6.2 Triaje y Verificación

> *CRA / prEN 40000-1-3 [VRF-1-RQ-01]: si el reporte inicial no contiene información suficiente para*

> *reproducir la vulnerabilidad, debe contactarse con quien reporta para solicitar detalles adicionales.*

Tras el acuse de recibo, el equipo de seguridad evalúa el reporte dentro del plazo definido. En esa evaluación, Wavecom procede a:

- Validar y reproducir las vulnerabilidades reportadas.
- Evaluar la gravedad mediante un sistema de puntuación establecido (CVSS v3.1).
- Identificar los productos y versiones afectados.
- Asignar prioridad y responsable de la corrección.

Si el reporte presentado no contiene información suficiente para reproducir la vulnerabilidad, el equipo de seguridad contactará con quien reporta para solicitar los detalles adicionales necesarios.

**WAVECOM** completa el triaje inicial y facilita información sobre el estado del proceso en un plazo de 7 días hábiles desde el acuse de recibo. Cuando el reporte se refiera a una vulnerabilidad explotada activamente, el triaje comienza de inmediato y el proceso de notificación del artículo 14 del CRA se activa en paralelo, con independencia de la comunicación con quien reporta.

## 6.3 Plazos de Corrección

> *prEN 40000-1-3 [RMD-2-RQ-01]: la corrección debe desarrollarse. [RMD-3-RQ-01]: la corrección debe probarse.*

**WAVECOM** trata de corregir las vulnerabilidades validadas dentro de los siguientes plazos objetivo, en función de la gravedad:

| Gravedad | Plazo objetivo |
|---|---|
| Crítica / alta (CVSS ≥ 7,0) | 30 días naturales |
| Media (CVSS 4,0 – 6,9) | 60 días naturales |
| Baja (CVSS < 4,0) | 90 días naturales |

| Gravedad | Plazo objetivo |
|---|---|
| Casos especiales (cuando proceda) | Equipos en campo que solo pueden actualizarse en una ventana de mantenimiento programada y vulnerabilidades en componentes de terceros a la espera de corrección del proveedor. Los plazos ampliados se acuerdan previamente con quien reporta, se justifican por escrito y se registran. |

**Escala de Gravedad y Tiempos de Respuesta**

| BAJA | MEDIA | ALTA | CRÍTICA |
|---|---|---|---|
| CVSS 0,1–3,9<br>Plazo objetivo:<br>90 días | CVSS 4,0–6,9<br>Plazo objetivo:<br>60 días | CVSS 7,0–8,9<br>Plazo objetivo:<br>30 días | CVSS 9,0–10,0<br>Plazo objetivo:<br>30 días* |

** Las vulnerabilidades críticas bajo explotación activa se priorizan para la corrección más rápida posible, incluso por delante del plazo objetivo de 30 días.*

Cuando la corrección no pueda entregarse dentro del plazo objetivo, Wavecom informará previamente a quien reporta, con una fecha revisada y, si las hubiera, orientaciones de mitigación provisional.

> *CRA / prEN 40000-1-3 [RMD-3-RQ-01]: la corrección debe probarse antes de su publicación para confirmar que resuelve la vulnerabilidad y no introduce nuevos problemas.*

Antes de publicar cualquier corrección, verificamos que resuelve la vulnerabilidad reportada y que no introduce nuevas debilidades de seguridad. En las vulnerabilidades de gravedad crítica y alta, las pruebas incluyen verificación funcional y, cuando proceda, pruebas de regresión.

## 6.4 Divulgación Pública Coordinada

Practicamos la divulgación coordinada: colaboramos con quien reporta la vulnerabilidad para acordar la fecha de publicación de la información, una vez disponible la corrección.

> *CRA — anexo I, parte II, punto (4): la información sobre vulnerabilidades corregidas debe divulgarse públicamente, incluidas descripción, versiones afectadas, gravedad y orientaciones de corrección. prEN 40000-1-3 [PRE-2-RC-02]: la política debe incluir el procedimiento de publicación. [PRE-2-RC-03]: la divulgación debe coordinarse para evitar una publicación prematura.*

**WAVECOM** trata de completar la divulgación coordinada en un plazo de 90 días naturales desde la fecha del acuse de recibo. Cuando no sea posible, contactamos con quien reporta antes del vencimiento para acordar una nueva fecha.

**Importante — derecho de divulgación:** cuando sea necesario para proteger a los usuarios o para cumplir obligaciones legales aplicables, **WAVECOM** se reserva el derecho de divulgar públicamente información sobre la vulnerabilidad sin el acuerdo previo ni la participación de quien reporta.

Cuando ambas partes acuerden un periodo de embargo — periodo durante el cual ninguna publicará información sobre la vulnerabilidad — el periodo acordado y su fecha de fin (fecha de divulgación) se documentarán por escrito. Cualquiera de las partes podrá solicitar una prórroga del embargo con justificación razonable.

Una vez publicada la corrección, Wavecom:

- Informa a quien reporta de que la vulnerabilidad ha sido resuelta.
- Publica un aviso de seguridad, nota de versión o notificación de producto.
- Acredita a quien reporta en el aviso público, con su consentimiento.

## 7. Plataforma Única de Notificación (SRP)

> *Información adicional: Reglamento (UE) 2024/2847, EUR-Lex, considerando (65).*

**Definiciones**

Vulnerabilidad explotada activamente: incidente de seguridad en el que un actor malicioso explota una vulnerabilidad activa del producto.

Incidente grave: incidente de seguridad en el que las funciones de seguridad del producto se ven afectadas de forma significativa y que no puede clasificarse como «vulnerabilidad explotada activamente».

## 7.1 Mecanismos de recopilación de información

| Canal | Definición | Detalle |
|---|---|---|
| Consultas a clientes | Se consulta periódicamente a los clientes sobre incidentes de seguridad que afecten a los productos. | Responsable: Departamento Comercial y Soporte Técnico. La seguridad se incluye en las revisiones periódicas de servicio al cliente y en las intervenciones en campo. Los registros se mantienen en el repositorio de incidentes; cualquier indicio de explotación se escala de inmediato al ISM. |
| Threat Intelligence | Vigilancia de fuentes comerciales y abiertas sobre explotación de vulnerabilidades | Avisos del CNCS y del CERT.PT, publicaciones de ENISA, feeds de CVE correlacionados con el inventario de componentes (SBOM) de WaveOS y de las plataformas (IoT Manager, CAS y WHERE IS) y boletines de proveedores y socios ODM/OEM (RAK, Supermicro, Kontron, Quectel, SimCom y proveedores de nube). |
| Presentación de vulnerabilidades | Evaluación de las vulnerabilidades recibidas por los canales de reporte para determinar si están siendo explotadas activamente. | Los reportes recibidos en ciberseguranca@wavecom.pt al amparo de esta política son triados por el ISM, que determina si existe evidencia fiable de explotación activa. |
| Gestión interna de vulnerabilidades | Evaluación de las vulnerabilidades identificadas internamente para determinar si están siendo explotadas activamente | Los resultados del ciclo de desarrollo seguro (SGSI_PLT10), de las pruebas internas y de terceros y de la monitorización y revisión de registros de las plataformas SaaS (IoT Manager, CAS, WHERE IS®) se evalúan en busca de evidencia de explotación activa. |
| Otros | | Escalado interno: todo empleado, contratista o ingeniero de campo que reciba un indicio de explotación activa lo comunica de inmediato al ISM, por escrito, sin evaluación técnica previa y sin filtrado jerárquico. |

## 7.2 Notificaciones a ENISA

Las notificaciones siguientes se presentan en la plataforma única de notificación de ENISA:

- https://portal.cra-srp.enisa.europa.eu/

| Tipo de notificación | Plazo (desde la detección) | Contenido de la notificación |
|---|---|---|
| Alerta temprana | 24 h | Tipo de notificación (vulnerabilidad / incidente)<br>Nivel de notificación (24 h, 72 h, final)<br>Nombre del fabricante o administrador<br>Producto<br>Título |
| Notificación de vulnerabilidad / incidente | 72 h | Contenido de la alerta temprana<br>Naturaleza de la vulnerabilidad<br>Naturaleza de la explotación<br>Medidas correctivas o de mitigación adoptadas<br>Medidas correctivas o de mitigación que pueden adoptar los usuarios<br>Sensibilidad de la información (cuando proceda) |
| Informe final (vulnerabilidades) | 14 días | Contenido de la notificación de vulnerabilidad / incidente<br>Fecha de disponibilidad de la medida correctiva o de mitigación<br>Descripción completa de la vulnerabilidad<br>Gravedad de la vulnerabilidad<br>Impacto de la vulnerabilidad<br>Actor malicioso que ha explotado la vulnerabilidad<br>Detalle de la actualización de seguridad / medidas correctivas disponibles |
| Informe final (incidentes graves) | 1 mes | Contenido de la notificación de vulnerabilidad / incidente<br>Descripción detallada del incidente<br>Gravedad del incidente<br>Impacto del incidente<br>Tipo de amenaza o causa raíz que ha originado el incidente<br>Medidas de mitigación aplicadas y en curso |

## 8. Confidencialidad y Reportes Anónimos

> *prEN 40000-1-3 [PRE-5-RC-03]: quien reporta debe poder presentar reportes de forma anónima.*

Todos los reportes de vulnerabilidad se tratan de forma confidencial. La información personal facilitada por quien reporta no se comparte con terceros sin consentimiento expreso, salvo cuando lo exija la legislación aplicable.

Quien desee mantener el anonimato puede presentar reportes por cualquiera de los canales indicados sin facilitar datos personales. Conviene tener en cuenta que el anonimato puede limitar nuestra capacidad de informar sobre el estado del proceso o de otorgar reconocimiento formal.

Los reportes anónimos se aceptan y se trían en los mismos términos que los reportes identificados. Si no se facilitan datos de contacto, no es posible solicitar aclaraciones, acordar una fecha de divulgación coordinada ni informar sobre el estado del proceso.

## 9. Información de Contacto

| Campo | Detalle |
|---|---|
| Contacto de seguridad | ciberseguranca@wavecom.pt |
| Dirección postal | WAVECOM – Soluções Rádio, S.A.<br>Rua das Cardadeiras, 107<br>3800-125 Aveiro, Portugal |
| Clave pública PGP | Disponible a petición. |
| Horario de respuesta | 09:00–18:00 (Europa/Lisboa), de lunes a viernes, salvo festivos en Portugal. Los reportes que indiquen explotación activa se escalan fuera de este horario a través del contacto de escalado permanente. |
| Contacto de escalado | Information Security Manager (ISM), como punto de contacto único CRA. Los contactos de escalado están documentados en SGSI_PLT19 (Lista de Contactos de Autoridades). |

# 10. Gestión de la Política

## 10.1 Revisión y Actualización

Esta política se revisa al menos anualmente, o antes ante cualquier cambio significativo de la gama de productos, del equipo de seguridad o del entorno regulatorio. Las versiones actualizadas se publican en el sitio web de Wavecom y se comunican internamente.

| Campo | Wavecom |
|---|---|
| ¿Dónde se publicará esta política? | https://www.wavecom.pt/security (por confirmar), con un fichero security.txt en https://www.wavecom.pt/.well-known/security.txt y una referencia en la documentación del producto. |
| ¿Quién es responsable de su revisión? | Information Security Manager (ISM) |
| Próxima revisión | Septiembre de 2027, o antes ante un cambio significativo del producto o del marco CRA aplicable |

## 10.2 Excepciones

Toda excepción a esta política debe ser aprobada por el propietario del documento y registrada en el registro de excepciones. Todas las excepciones son temporales y se revisan anualmente.

# 11. Historial del Documento

| Versión | Fecha | Autor | Descripción del cambio |
|---|---|---|---|
| 1.0 | 8 de septiembre de 2026 | Information Security Manager (ISM) | Versión inicial, adaptada de la plantilla de política CVD de Eurofins v1.0 |