

SEGURIDAD DE PRODUCTO

Reglamento de Ciberresiliencia (CRA) y seguridad de producto

Reglamento (UE) 2024/2847

COMPROMISO CON LA CIBERSEGURIDAD

MACSA ID se compromete a desarrollar y mantener productos y servicios seguros de acuerdo con las buenas prácticas de ciberseguridad reconocidas y con los requisitos del Reglamento de Ciberresiliencia de la UE (Reglamento (UE) 2024/2847). La seguridad de nuestros clientes, socios y usuarios es un elemento central del ciclo de vida de nuestros productos.

SEGURIDAD DESDE EL DISEÑO

La seguridad está integrada en todas las fases de diseño, desarrollo, pruebas, despliegue y mantenimiento de nuestros productos.

Nuestras prácticas de seguridad incluyen:

- Procesos de desarrollo seguro
- Evaluaciones de seguridad basadas en el riesgo
- Gestión y corrección de vulnerabilidades
- Pruebas y validación de seguridad
- Publicación controlada de actualizaciones de seguridad
- Seguimiento continuo de las amenazas de seguridad relevantes

Estas medidas nos ayudan a identificar, evaluar y reducir los riesgos de ciberseguridad a lo largo de todo el ciclo de vida del producto.

NOTIFICACIÓN DE VULNERABILIDADES

Agradecemos las notificaciones de investigadores de seguridad, clientes y socios que detecten posibles vulnerabilidades de seguridad en nuestros productos o servicios.

Para notificar una vulnerabilidad, póngase en contacto con:

EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE
PRODUCTO (PSIRT)

psirt@macsa.com

La información debe enviarse en español o en inglés.

Para que podamos evaluar y tramitar la notificación lo antes posible, incluya en ella la siguiente información:

- 1 Nombre del producto, modelo y número de serie.
- 2 Versión y configuración del software o firmware.
- 3 Una descripción clara y detallada de la vulnerabilidad o el problema detectado.
- 4 Los pasos para reproducirlo.
- 5 Evidencias que faciliten la validación (por ejemplo, detalles de configuración, capturas de pantalla, registros o información sobre cómo explotar la vulnerabilidad).
- 6 Una valoración del impacto potencial.
- 7 Datos de contacto para el seguimiento del caso.

MACSA ID respeta la confidencialidad de quienes envían notificaciones y no revelará sus datos personales sin su consentimiento explícito, salvo que sea necesario para gestionar la vulnerabilidad.

POLÍTICA DE DIVULGACIÓN COORDINADA DE VULNERABILIDADES

Apoyamos la divulgación responsable y coordinada de vulnerabilidades.

Al recibir una notificación de vulnerabilidad, nos proponemos:

- 1 Acusar recibo de la notificación.
- 2 Evaluar y validar el problema notificado.
- 3 Determinar las medidas de corrección adecuadas.
- 4 Coordinar la comunicación con la persona que lo ha notificado, cuando proceda.
- 5 Informar a los usuarios afectados y publicar información de seguridad cuando sea pertinente.

Pedimos a los investigadores que:

- Actúen de buena fe.
- Eviten acceder a datos, modificarlos o eliminarlos.
- Eviten interrumpir servicios o sistemas.
- Concedan un plazo razonable para la corrección antes de cualquier divulgación pública.

El objetivo de este proceso es proteger a los usuarios y garantizar que las vulnerabilidades se corrijan de forma responsable.

INFORMACIÓN DE SEGURIDAD

La información de seguridad vigente puede incluir:

- Avisos de seguridad
- Notificaciones de vulnerabilidades
- Comunicados de seguridad de producto
- Información sobre actualizaciones y parches
- Datos de contacto de seguridad de producto