POLÍTICA DE SEGURIDAD

NanoFactura y Asistente Factura Electrónica

Versión 2026.1

Fecha de última actualización: 1 de agosto de 2026 **Fecha de entrada en vigencia:** 1 de agosto de 2026

Esta Política de Seguridad complementa los Términos y Condiciones, la Política de Privacidad y la Política de Cookies de NanoFactura (versión 2026.1) y utiliza los mismos términos definidos en ellos. Su objeto es describir, en términos generales, las medidas y buenas prácticas que la Plataforma aplica para proteger la información, vigentes al momento de su publicación, así como el modo en que se pueden reportar posibles vulnerabilidades.

NanoFactura es la plataforma y servicio principal; la extensión para navegador **Asistente Factura Electrónica**, el sitio web y la API son sus **Canales Oficiales**. La presente Política se aplica por igual a la utilización de los Servicios a través de cualquiera de ellos.

Control de versiones

Versión	Fecha	Descripción
2026.1	15/07/2026	Primera Política de Seguridad de NanoFactura.

Índice

---

1. Alcance y compromiso

El Prestador aplica medidas técnicas y organizativas razonables para proteger la información tratada a través de la Plataforma frente al acceso no autorizado, la pérdida, la alteración o la divulgación indebida.

La seguridad es un proceso continuo. El Prestador revisa y actualiza sus prácticas de manera periódica, en función de la evolución tecnológica, de los riesgos identificados y de las mejores prácticas de la industria.

---

2. Cifrado y protección de la información

Las comunicaciones entre los dispositivos de los Usuarios y la Plataforma se realizan a través de conexiones cifradas (**HTTPS/TLS**).

La información sensible almacenada en la infraestructura de la Plataforma —en particular los Certificados Digitales— se conserva **cifrada**. El acceso a la información se limita al mínimo necesario para prestar los Servicios.

---

3. Certificados Digitales

Los Certificados Digitales de ARCA y sus componentes asociados (clave privada, CSR, alias, frase de acceso, datos de vencimiento y tokens temporales) se almacenan cifrados y se tratan con la finalidad exclusiva de habilitar la interacción con ARCA.

El acceso a los Certificados Digitales se restringe a los **procesos automáticos** de la Plataforma necesarios para prestar los Servicios, **sin acceso humano rutinario**. Excepcionalmente podrá existir acceso cuando resulte estrictamente necesario para tareas de soporte, investigación de incidentes, cumplimiento de obligaciones legales o mantenimiento de la Plataforma, conforme a los Términos y Condiciones. El acceso con fines de soporte se rige por la Sección 15.4 de los Términos y Condiciones.

---

4. Autenticación y control de acceso

El acceso interactivo a los Servicios se realiza mediante **proveedores de autenticación administrados por terceros**, actualmente Google mediante Firebase Authentication. El acceso programático, en los Planes que lo habiliten, se realiza mediante **API Keys generadas por NanoFactura**.

El Prestador procura aplicar el principio de **mínimo privilegio**, limitando los accesos internos a la información y a los sistemas a lo estrictamente necesario para cada función.

---

5. Credenciales y API Keys

Las Credenciales y API Keys son mecanismos de acceso cuya confidencialidad debe preservarse. El Prestador puede:

- establecer cuotas de uso y límites de frecuencia (rate limits) sobre la API;
- suspender o revocar API Keys ante motivos razonables de seguridad, uso indebido o afectación de la estabilidad de la Plataforma;
- regenerarlas cuando resulte necesario por motivos de seguridad.

El Usuario es responsable de la custodia de sus Credenciales y API Keys y de todo uso que se realice a través de ellas, conforme a los Términos y Condiciones.

---

6. Minimización de datos

La Plataforma se rige por el principio de minimización: solo se almacena en su infraestructura la información necesaria para prestar los Servicios contratados.

En **determinados Planes**, gran parte de la información operativa permanece en el dispositivo del Usuario y no se sincroniza con la infraestructura del Prestador. Esta arquitectura reduce la superficie de exposición: el Prestador no puede acceder a información que nunca fue transmitida a su infraestructura.

7. Infraestructura y continuidad

La Plataforma se apoya en proveedores de infraestructura y servicios que aplican estándares de seguridad reconocidos. El Prestador podrá realizar copias de resguardo (backups) de la información almacenada en su infraestructura, con el fin de contribuir a su disponibilidad y recuperación ante incidentes.

Los proveedores que actúan como encargados del tratamiento se detallan en la Política de Privacidad.

8. Registro y monitoreo

Con el objeto de detectar incidentes, prevenir fraudes, mantener la estabilidad de la Plataforma y mejorar la seguridad de los Servicios, el Prestador podrá registrar eventos técnicos, accesos, errores, actividad de autenticación y otros registros operativos.

Estos registros serán tratados conforme a la Política de Privacidad y conservados únicamente durante el tiempo necesario para las finalidades indicadas.

9. Responsabilidades del Usuario

La seguridad es una responsabilidad compartida. Se recomienda al Usuario:

- proteger las Credenciales de su cuenta de autenticación y no compartirlas;
- custodiar sus API Keys y revocarlas ante cualquier sospecha de compromiso;
- mantener actualizados su navegador y su dispositivo;
- verificar que accede a los Servicios únicamente a través de los Canales Oficiales;
- comunicar al Prestador, sin demoras indebidas, cualquier incidente de seguridad del que tome conocimiento.

10. Gestión de incidentes

Ante un incidente de seguridad que pueda afectar la información de los Usuarios, el Prestador procurará adoptar las medidas razonables para contenerlo, evaluar su alcance y mitigar sus efectos, así como informar a los Usuarios y a las autoridades cuando ello resulte exigible conforme a la legislación aplicable.

La existencia de un incidente de seguridad no implica por sí misma responsabilidad del Prestador, la cual se regirá por los Términos y Condiciones y la legislación aplicable.

11. Divulgación responsable de vulnerabilidades

El Prestador valora la colaboración de la comunidad de seguridad. Si un investigador o Usuario detecta una posible vulnerabilidad, se solicita reportarla de manera responsable a través del correo de contacto indicado en la Sección 13, incluyendo la información necesaria para reproducirla.

Se solicita, asimismo:

- no acceder, modificar ni divulgar información de otros Usuarios;
- no degradar ni interrumpir el funcionamiento de los Servicios;
- otorgar un plazo razonable para su resolución antes de cualquier divulgación pública.

El Prestador se compromete a analizar los reportes recibidos de buena fe y a no promover acciones contra quienes actúen de forma responsable, ajustándose a estas pautas y a la legislación aplicable.

El envío de un reporte no genera derecho a compensaciones, recompensas o reconocimiento económico, salvo acuerdo expreso del Prestador.

12. Limitaciones

Ningún sistema, producto o servicio es completamente infalible. Si bien el Prestador aplica medidas de seguridad razonables, no garantiza una seguridad absoluta ni la imposibilidad de incidentes.

Esta Política describe prácticas generales y no crea obligaciones de resultado ni niveles de servicio garantizados, sin perjuicio de las obligaciones legales que resulten aplicables y de lo previsto en los Términos y Condiciones y en la Política de Privacidad.

---

13. Modificaciones y contacto

El Prestador podrá modificar la presente Política de Seguridad para adecuarla a cambios legales, tecnológicos o funcionales. Las nuevas versiones serán publicadas en los Canales Oficiales e indicarán su fecha de entrada en vigencia.

Para reportar vulnerabilidades o realizar consultas de seguridad, el Usuario podrá comunicarse con el Prestador, **Mariano Oscar Paulin** (CUIT 20-38373889-0), titular de la marca registrada **NanoFactura**, a través de:

Domicilio electrónico constituido: contacto@nanofactura.com o contacto@asistentefacturaelectronica.com

Jurisdicción: Provincia de Santa Fe, República Argentina. El domicilio postal completo se encuentra a disposición del Usuario y de la autoridad competente que lo requiera, a través de los medios de contacto indicados.

Esta Política de Seguridad complementa los Términos y Condiciones, la Política de Privacidad y la Política de Cookies de NanoFactura (versión 2026.1). En caso de discrepancia entre versiones traducidas, prevalecerá la versión redactada en idioma español.