



República de Panamá
AUTORIDAD NACIONAL PARA LA INNOVACION GUBERNAMENTAL

Resolución No. 36
de 13 de agosto de 2026

"Por la cual se aprueba la **GUÍA DE APLICACIÓN DE LA RESOLUCIÓN NO. 18 DE 15 DE JUNIO DE 2026, PARA LA EVALUACIÓN Y AUTORIZACIÓN DE LA PUESTA EN PRODUCCIÓN DE PLATAFORMAS DIGITALES CON ACCESO O INTERACCIÓN CIUDADANA**".

El Administrador General de la Autoridad Nacional para la Innovación Gubernamental,
en uso de sus facultades legales,

CONSIDERANDO:

Que mediante la Ley 65 de 30 de octubre de 2009, se creó la Autoridad Nacional para la Innovación Gubernamental (AIG), como una entidad del Estado con personería jurídica, patrimonio propio y autonomía en su régimen interno, con capacidad de adquirir derechos y contraer obligaciones, administrar sus bienes y gestionar sus recursos, competente para planificar, coordinar, emitir directrices, supervisar, colaborar, apoyar y promover el uso óptimo de las tecnologías de la información y comunicaciones en el sector gubernamental, para la modernización de la gestión pública.

Que entre las funciones de la AIG, está la de coordinar el desarrollo de iniciativas relacionadas con el uso de las Tecnologías de la Información y Comunicaciones (TIC) a ser utilizadas por parte de las entidades públicas con la ciudadanía, facilitando sus trámites y servicios gubernamentales, de manera que esto conlleve a la modernización del Estado, mediante la transformación digital y el uso de herramientas tecnológicas, con particular énfasis en proyectos que tiendan a mejorar la eficiencia y calidad de los servicios gubernamentales.

Que mediante la Resolución No. 18 de 15 de junio de 2026, la Autoridad Nacional para la Innovación Gubernamental estableció que las plataformas digitales con acceso o interacción ciudadana, a ser desarrolladas o gestionadas por las instituciones del Estado, deberán ser sometidas a evaluación y autorización previa por parte de esta Autoridad antes de su puesta en producción, estableciendo para tal efecto los requisitos y el procedimiento que deberán cumplir las entidades responsables para la presentación de las solicitudes correspondientes.

Que, en atención a las competencias de rectoría de la Autoridad Nacional para la Innovación Gubernamental en materia de innovación gubernamental y tecnologías de la información y las comunicaciones, resulta necesario establecer criterios y lineamientos que faciliten a las entidades del Estado la correcta aplicación de las disposiciones contenidas en la Resolución No. 18 de 15 de junio de 2026.

Que, en virtud de lo anterior, resulta procedente aprobar la Guía de Aplicación de la Resolución No. 18 de 15 de junio de 2026, como instrumento técnico para la aplicación de las disposiciones contenidas en la referida Resolución, por lo que,

RESUELVE:

PRIMERO: APROBAR la "**GUÍA DE APLICACIÓN DE LA RESOLUCIÓN No. 18 DE 15 DE JUNIO DE 2026, PARA LA EVALUACIÓN Y AUTORIZACIÓN DE LA PUESTA EN**



Este documento es fiel copia del original, que reposa en la
Autoridad Nacional para la Innovación Gubernamental.

Firma:

[Firma manuscrita]



AK.

PRODUCCIÓN DE PLATAFORMAS DIGITALES CON ACCESO O INTERACCIÓN CIUDADANA”, que se adjunta a la presente Resolución.

SEGUNDO: ORDENAR la publicación de esta Resolución en Gaceta Oficial.

TERCERO: Esta Resolución rige a partir de su publicación en la Gaceta Oficial.

FUNDAMENTO DE DERECHO: Ley 65 de 30 de octubre de 2009, Texto Único de la Ley 22 de 2006, que regula la contratación pública, ordenado por la Ley 153 del 8 de mayo de 2020,Ley 38 de 31 de julio de 2000, Resolución No. 18 de 15 de junio de 2026.

PUBLIQUESE Y CUMPLASE,


ADOLFO FÁBREGA
Administrador General



Este documento es fiel copia del original, que reposa en la
Autoridad Nacional para la Innovación Gubernamental.

Firma:



GUÍA DE APLICACIÓN DE LA RESOLUCIÓN No. 18 DE 15 DE JUNIO DE 2026
Evaluación y autorización para la puesta en producción de plataformas digitales con acceso o interacción ciudadana
Versión 1.0 — Agosto de 2026

1. Objeto

La presente Guía tiene por objeto establecer los criterios técnicos, la clasificación de riesgo, los requisitos y el flujo procedimental que las instituciones del Estado deberán observar para obtener la evaluación y autorización de la Autoridad Nacional para la Innovación Gubernamental (AIG) previo a la puesta en producción de sus plataformas digitales, conforme a la Resolución No. 18 de 15 de junio de 2026 (Gaceta Oficial No. 30553-D).

La finalidad de esta Guía, es asegurar que las soluciones lleguen a producción con niveles verificables de seguridad, calidad funcional y desempeño, aplicando el principio de proporcionalidad: la profundidad de los controles exigidos será acorde al nivel de riesgo de cada plataforma.

2. Alcance

Quedan sujetas a esta Guía todas las plataformas digitales con acceso o interacción ciudadana que sean desarrolladas o gestionadas por las instituciones del Estado, con anterioridad a su puesta en producción. Se incluyen los desarrollos nuevos, así como las nuevas versiones o cambios mayores que modifiquen sustancialmente la funcionalidad, la superficie de exposición o el tratamiento de datos de una plataforma existente.

Los sistemas de uso exclusivamente interno, sin acceso ni interacción ciudadana, no se encuentran comprendidos en el alcance de la Resolución, sin perjuicio de las buenas prácticas de seguridad que cada entidad deba observar.

3. Base legal

- Ley 65 de 30 de octubre de 2009, que crea la Autoridad Nacional para la Innovación Gubernamental y le confiere la rectoría en materia de tecnologías de la información y comunicación en el sector gubernamental.
- Ley 81 de 26 de marzo de 2019, sobre protección de datos personales, en lo aplicable al tratamiento de datos por las plataformas evaluadas.
- Decreto Ejecutivo No. 719 de 15 de noviembre de 2013, modificado por el Decreto Ejecutivo No. 357 de 9 de agosto de 2016, en cuanto a la Agenda Digital Interinstitucional.



- Resolución No. 18 de 15 de junio de 2026, que establece la obligatoriedad de evaluación y autorización de las plataformas digitales previo a su puesta en producción.

4. Definiciones

- **Plataforma digital:** todo portal, aplicación o solución tecnológica accesible por el ciudadano por medio de un usuario identificado o que permita su interacción con la institución.
- **Acceso o interacción ciudadana:** la posibilidad de que el ciudadano consulte información personal o restringida se autentique, ingrese datos o ejecute trámites o transacciones en la plataforma.
- **Tercero independiente:** evaluador que no ha participado, directa ni indirectamente, en el desarrollo, la implementación o el mantenimiento de la solución evaluada.
- **Puesta en producción:** la habilitación de la plataforma para su uso real por parte de los usuarios finales.
- **Subsanación:** la corrección o complemento que la entidad realiza a su solicitud, a requerimiento de la AIG.

5. Clasificación de plataformas por nivel de riesgo

Toda entidad deberá clasificar su plataforma en una de las siguientes categorías. La categoría determina la profundidad de los requisitos exigibles (Sección 6). Ante la duda entre dos categorías, se adoptará la de mayor nivel.

Criterio	Categoría I (Informativa)	Categoría II (Interactiva / Transaccional)
Autenticación de usuarios	No	Sí
Tratamiento de datos personales	No captura datos	Datos personales, sensibles, financiero y/o de registros nacionales
Transacciones o pagos	No	Trámites / formularios / pagos / transacciones de alto impacto
Criticidad / disponibilidad	Baja	Media/Alta
Ejemplos	Portal informativo, micrositio de campaña, página de divulgación	Formulario de registro, cita en línea, registros sensitivos y/o pasarela de pagos



Facultad de reclasificación: La AIG se reserva la facultad de revisar la clasificación declarada por la entidad y de reclasificar la plataforma cuando, a su criterio técnico, el nivel de riesgo así lo amerite. La reclasificación podrá ajustar los requisitos exigibles conforme a la Sección 6.

6. Requisitos por categoría

Toda solicitud debe pronunciarse sobre las cuatro dimensiones establecidas en el Artículo 2 de la Resolución No. 18 de 15 de junio de 2026. La evidencia exigible en cada dimensión escala conforme a la categoría de la plataforma, según la siguiente matriz:

Requisito (Art. 2)	Categoría I	Categoría II
Validación de ciberseguridad por evaluador independiente	Verificación básica de seguridad (HTTPS, hardening, análisis de dependencias/SCA) declarada por la entidad	- Revisión de código manual o automatizada vía SAST + DAST. - Revisión de configuración cuando aplique.
Remediación de vulnerabilidades críticas y altas	Aplicable a los hallazgos que se detecten	Obligatoria, con evidencia
Pruebas funcionales	No obligatoria. Opcional acta de Aceptación del Usuario (UAT)	Acta de Aceptación (UAT)
Pruebas de carga y estrés	No obligatoria. Verificación básica de disponibilidad (interna)	Interna o especializada, según la demanda esperada
Integración con Panamá Conecta (Opcional en todo caso)	Enlace informativo, cuando aplique	SSO y enlace del trámite ("linked") o desarrollo directo sobre la plataforma de Panamá Conecta, así como integración de datos para el trámite o servicio
Justificación de no inclusión en Agenda Digital	Justificación simplificada (declaración breve)	Justificación

Nota: Todas las plataformas, sin distinción de categoría, deben aprobar exitosamente sus pruebas funcionales y remediar los hallazgos de seguridad críticos y altos que se identifiquen antes de la puesta en producción.



7. Presentación de la solicitud de evaluación para las plataformas digitales con acceso o interacción ciudadana.

La entidad responsable presentará ante la AIG una Solicitud de Evaluación acompañada del expediente que corresponda a la categoría de la plataforma. El medio para su presentación será la aplicación “SES – Sistema de Evaluación de Solicitudes”. La misma se ha extendido para poder recibir igualmente solicitudes de puesta en marcha de aplicaciones producto de la resolución 18 de 15 de junio de 2026. Su objetivo principal es asegurar que las iniciativas tecnológicas de las instituciones cumplan con criterios técnicos, normativos y de calidad antes de su ejecución, garantizando un uso eficiente y responsable de los recursos públicos, así como un alto nivel de calidad y seguridad en los servicios que despliega el Estado a la ciudadanía.

En casos donde en la aplicación SES – Sistema de Evaluación de Solicitudes no esté habilitado, la solicitud podrá presentarse mediante nota dirigida a la AIG, acompañada del expediente digital. La AIG dispondrá de un plazo de hasta quince (15) días para emitir su respuesta, conforme al Artículo 2 de la Resolución.

Carga de la documentación y seguimiento de la solicitud.

Para realizar la solicitud, la entidad deberá ingresar al Sistema de Evaluación de Solicitudes (SES) y cargar la información correspondiente del proyecto, incluyendo las evidencias o sustentación de cumplimiento de las pruebas de ciberseguridad, pruebas funcionales, etc. de acuerdo con lo establecido en la Resolución. No. 18 de 15 de junio de 2026 y la presente Guía.

A través del Sistema de Evaluación de Solicitudes (SES), la entidad recibirá las notificaciones correspondientes para atender las subsanaciones que sean requeridas o, en su defecto, la autorización de la AIG para la puesta en producción de la plataforma.

Contenido mínimo del informe de validación de ciberseguridad.

El informe que sustente la validación de ciberseguridad deberá contener, como mínimo:

- Alcance evaluado (aplicación, APIs, infraestructura y componentes en línea) y activos comprendidos.
- Metodología, estándares aplicados y tipos de prueba ejecutados.
- Inventario de hallazgos clasificados por severidad conforme a CVSS, con evidencia.
- Evidencia de corrección, mitigación y re-prueba de las vulnerabilidades críticas y altas.
- Declaración de Independencia del evaluador.
- Conclusión técnica de aptitud para la puesta en producción.

Estándares de referencia: OWASP ASVS y OWASP Web/API Security Testing Guide; NIST SP 800-115; ISO/IEC 27001 e ISO/IEC 27002; y CIS Benchmarks para aseguramiento (hardening).



AF.

8. Evaluador independiente y uso de herramientas institucionales.

El requisito de independencia se satisface con cualquiera de estas modalidades, siempre que el evaluador no haya participado en el desarrollo, la implementación o el mantenimiento de la solución: (i) una unidad interna de la entidad, funcionalmente separada del equipo de proyecto; (ii) otra entidad del Estado con capacidad especializada; o (iii) una empresa externa contratada para tal fin.

El análisis estático de código (SAST) ejecutado con herramientas especializadas se considera una evaluación independiente, por cuanto las reglas y parametrizaciones de detección constituyen un marco de verificación creado por un tercero, ajeno al equipo de desarrollo. Su informe nativo, complementado con el informe institucional de remediación, constituye evidencia válida.

No obstante, y aun cuando no sea exigible, es responsabilidad de cada entidad asegurar el nivel de verificación más adecuado a la criticidad de la solución y de sus datos; por ello se recomienda complementar el análisis con una evaluación más profunda, que podrá ser ejecutada por un tercero independiente. Cuando la entidad no cuente con el personal para ello, la AIG podrá considerar la realización de una revisión con personal propio, previa coordinación.

La evaluación independiente complementa —no sustituye— los controles internos de seguridad de la institución, en un esquema de defensa en capas.

En particular, el proveedor que haya desarrollado, implementado o mantenga la solución no puede autoevaluarse: por tratarse de una parte vinculada al desarrollo, no califica como evaluador independiente respecto de su propio trabajo. Por ello, la validación independiente debe preverse desde la contratación del proyecto.

9. Pruebas de carga, estrés y funcionales.

Las pruebas de carga, estrés y funcionales podrán ser ejecutadas por el personal técnico interno de la institución (incluidas las áreas de Aseguramiento de la Calidad) o por un proveedor especializado; no requieren ser ejecutadas por el tercero independiente de ciberseguridad. Los reportes internos de QA son válidos como evidencia siempre que sean trazables y documenten escenarios, condiciones máximas previstas, resultados y criterios de aceptación.

En materia funcional, el Acta de Aceptación del Usuario (UAT) es suficiente como evidencia de la culminación exitosa de las pruebas funcionales; para las categorías II y III se acompañará de la matriz de casos de prueba correspondiente.

10. Agenda Digital Interinstitucional (Artículo 3).

Cuando la plataforma no se encuentre contemplada en la Agenda Digital de la institución, la entidad deberá presentar la debida justificación de su no inclusión. Dicha justificación podrá consistir en una declaración breve del motivo de la no inclusión, sin perjuicio de su posterior incorporación a la Agenda Digital en el ciclo que corresponda.



AF.

11. Integración con el programa Panamá Conecta (Artículo 4).

Panamá Conecta constituye la plataforma para la unificación de la tramitología del Estado de cara al ciudadano, y forma parte de la hoja de ruta digital presentada en Consejo de Gabinete a inicios del año 2025 y a los directores de tecnología Institucionales en el mismo año. No debe interpretarse de forma taxativa que toda plataforma deba integrarse obligatoriamente, en todos sus componentes, al programa; el principio rector es la interoperabilidad y la experiencia unificada del ciudadano.

Existen distintas modalidades de integración, con niveles de esfuerzo escalonados:

- **Integración nativa:** la solución utiliza el inicio de sesión único de Panamá Conecta y el trámite se realiza sobre la plataforma o Motor Multi-trámite (MMT) de Panamá Conecta.
- **Autenticación única (SSO):** la solución utiliza el inicio de sesión único de Panamá Conecta y el trámite queda enlazado ("linked") desde la plataforma.
- **Enlace informativo:** cuando el SSO no sea viable o la plataforma sea informativa, bastará con enlazarla, junto con la información de su existencia, para que el ciudadano pueda ubicarla desde Panamá Conecta.

La integración a Panamá Conecta es opcional como decisión propia de la entidad que realiza el proyecto y el objetivo que se busca con la justificación es conocer las razones de una decisión y asegurar que la integración a Panamá Conecta haya sido considerada. La AIG evaluará las justificaciones de no integración caso por caso, conforme al Artículo 4 de la Resolución.

12. Flujo procedimental, subsanaciones y plazos.

- **Presentación:** la entidad presenta la Solicitud de Evaluación con el expediente correspondiente a su categoría.
- **Evaluación de la AIG:** la AIG se pronuncia dentro de un plazo de hasta quince (15) días, autorizando la puesta en producción o emitiendo nota de subsanación bajo fundamento técnico.
- **Plazo de subsanación de la entidad:** es indefinido; la entidad presenta la subsanación cuando esta se encuentre lista, sin que ello genere caducidad de la solicitud.
- **Plazo de la AIG en cada subsanación:** cada subsanación presentada tendrá un plazo máximo de quince (15) días de respuesta por parte de la AIG; este plazo aplica a la Autoridad y no constituye límite para la entidad.

Sistema de gestión: para la tramitación de estas solicitudes se adoptará el Sistema de Evaluación de Solicitudes (SES), cuyo procedimiento y flujo de uso se detallarán como parte de esta Guía.



AF.

Puesta en producción sin autorización: conforme al Artículo 5 de la Resolución, queda prohibida la puesta en producción de plataformas que no cuenten con la autorización de la AIG; su incumplimiento podrá dar lugar a la suspensión temporal o definitiva de la operación.

13. Sistemas en producción a la fecha de entrada en vigencia de la Resolución.

Las plataformas digitales que ya se encontraban en producción a la fecha de entrada en vigencia de la Resolución No. 18 de 15 de junio de 2026, no requieren someterse a un nuevo proceso de evaluación y autorización por ese solo hecho, y podrán continuar en operación normal. No corresponde acción alguna respecto de dichas plataformas por su condición de existentes.

No obstante, la entidad responsable deberá mantener sobre ellas las labores de mantenimiento, actualización y pruebas constantes de validación de seguridad propias de su ciclo de vida. La obligación de evaluación y autorización previa aplicará únicamente cuando dichas plataformas sean objeto de un cambio mayor, conforme a la Sección 14.

14. Cambios mayores y vigencia de la autorización.

Cambio mayor

Se entiende por cambio mayor toda modificación sustancial de una plataforma, tal como un cambio completo de versión, la incorporación de nuevas funcionalidades transaccionales, cambios importantes en la estructura de datos o en el stack tecnológico, u otros de naturaleza equivalente.

Igualmente, se considera cambio mayor un sitio web informativo que pasa a tener una funcionalidad transaccional.

Queda a criterio y responsabilidad de la entidad determinar cuándo un cambio constituye un cambio mayor y, en consecuencia, informarlo a la AIG y someterlo a evaluación conforme a esta Guía.

Vigencia de la autorización

La autorización emitida por la AIG tiene vigencia permanente, en tanto la plataforma no sea objeto de un cambio mayor. La ocurrencia de un cambio mayor obliga a una nueva evaluación y autorización respecto de la versión modificada.

15. Responsabilidad de la entidad.

La responsabilidad sobre el desarrollo, la operación, el mantenimiento, la disponibilidad y la protección de los datos de cada plataforma corresponde íntegramente a la entidad titular. La evaluación y autorización de la AIG no constituye un traspaso ni una asunción de dicha responsabilidad por parte de la Autoridad: la AIG se limita a validar que se cumplieron los procedimientos de calidad y seguridad establecidos para la puesta en marcha.



Handwritten signature or mark.

En consecuencia, la autorización no exime a la entidad de sus obligaciones ni de las responsabilidades derivadas de la operación de su plataforma.

16. Costos de los ejercicios de validación.

Los costos en que la entidad incurra para cumplir con los ejercicios de validación previstos en esta Guía —incluidas las pruebas de ciberseguridad, funcionales y de carga y estrés— no son contemplados ni asumidos por la AIG. Dichos costos deben ser previstos por la entidad dentro del presupuesto del proyecto respectivo, como trabajos básicos y críticos de validación inherentes a toda puesta en marcha y al ciclo de vida del software.

Por ello, se recomienda incorporar estos requisitos, y la validación independiente cuando corresponda, desde la etapa de planificación y contratación del proyecto.

17. Obligaciones complementarias.

El cumplimiento de esta Guía no reemplaza ni exime del cumplimiento de las demás obligaciones legales y técnicas vigentes aplicables a la plataforma, entre ellas:

- La protección de datos personales, conforme a la Ley 81 de 2019.
- La gestión continua de vulnerabilidades y actualizaciones de seguridad a lo largo del ciclo de vida.
- Las normas de interoperabilidad y de accesibilidad que resulten aplicables.
- Las directrices técnicas emitidas por la AIG.

La validación previa a la puesta en producción es un requisito adicional y concurrente con dichas obligaciones, no sustitutivo de ellas.

A. Anexo — Ejemplo de aplicación: sitio web informativo (Categoría I).

Caso: una entidad requiere publicar un sitio web de carácter informativo, de contenido estático, sin autenticación de usuarios, que no captura datos personales ni ejecuta trámites o transacciones. Aplicación de la Guía:

- **Clasificación:** Categoría I (Informativa).
- **Validación de ciberseguridad:** verificación básica de seguridad declarada por la entidad (HTTPS, hardening del servidor, análisis de dependencias). No se requiere contratar pruebas de penetración por tercero externo.
- **Pruebas de carga y estrés:** no obligatorias; basta una verificación básica de disponibilidad realizada internamente. No se requiere contratar un servicio especializado.
- **Pruebas funcionales:** Acta de Aceptación del Usuario (UAT).



AF.

- **Agenda Digital:** si no estaba incluida, se presenta una justificación simplificada de no inclusión.
- **Panamá Conecta:** no requiere integración transaccional; a lo sumo, un enlace informativo desde Panamá Conecta.

En consecuencia, un sitio de esta naturaleza puede completar su solicitud sin necesidad de procesos de contratación de pentest o de pruebas de estrés, atendiendo la premura de su publicación.

Anexo B — Ejemplo de aplicación: plataforma de despliegue de subsidios (Categoría III).

Caso: una entidad requiere poner en producción una plataforma que autentica al ciudadano, consulta y almacena datos personales y financieros, valida elegibilidad contra registros nacionales y ejecuta la dispersión de subsidios mediante transacciones de pago.

Aplicación de la Guía:

Clasificación: Categoría III (Crítica), por concurrir autenticación de usuarios, tratamiento de datos personales y financieros, ejecución de transacciones de pago y alta criticidad/disponibilidad. Ante la concurrencia de varios factores de riesgo, se adopta la categoría de mayor nivel.

Validación de ciberseguridad: se requiere un informe de alcance completo emitido por un tercero independiente, que abarque análisis estático (SAST), análisis dinámico (DAST), pruebas de penetración autenticadas y no autenticadas, seguridad de APIs, revisión de configuración y aseguramiento (hardening), y análisis de composición de software (SCA). El informe debe clasificar los hallazgos por severidad conforme a CVSS y adjuntar la declaración de independencia del evaluador.

Remediación de vulnerabilidades críticas y altas: obligatoria, con evidencia de corrección y de re-prueba (re-test) documentada para cada hallazgo crítico y alto, previo a la puesta en producción.

Pruebas funcionales: Acta de Aceptación del Usuario (UAT), acompañada de la matriz de casos de prueba ejecutados con sus resultados y de la cobertura de los requisitos funcionales, incluidos los flujos de elegibilidad, cálculo y dispersión.

Pruebas de carga y estrés: obligatorias, ejecutadas bajo condiciones máximas y realistas de uso (usuarios concurrentes en picos de dispersión, transacciones por segundo, tiempos de respuesta, tasa de error y consumo de recursos), con criterios de aceptación definidos.

Protección de datos: por tratar datos personales y financieros, deberá evidenciarse el cifrado en tránsito y en reposo, la gestión de secretos y los controles de acceso, en concordancia con la Ley 81 de 2019.



Handwritten signature

Agenda Digital: deberá estar incluida en la Agenda Digital de la institución; de no estarlo, se presenta la justificación formal de no inclusión.

Panamá Conecta: requiere integración mediante autenticación única (SSO) e integración del trámite o servicio de dispersión, al tratarse de una transacción ciudadana directa.

En consecuencia, una plataforma de esta naturaleza no puede ser puesta en producción sin la validación completa por tercero independiente, la remediación verificada de los hallazgos críticos y altos, y las pruebas de carga y estrés correspondientes, dado el impacto de una falla sobre los datos y los recursos dispersados al ciudadano.

