República de Panamá

AUTORIDAD NACIONAL PARA LA INNOVACION GUBERNAMENTAL

Resolución No. 07
11 de mayo de 2026

"Por la cual se establecen los controles mínimos requeridos de Protección en Ciberseguridad para los Sistemas Informáticos de las Entidades Públicas"

El suscrito Administrador General de la Autoridad Nacional para la Innovación Gubernamental

En uso de sus facultades legales, y

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 autónoma con patrimonio propio, personería jurídica, autonomía en su régimen interno, con capacidad de adquirir derechos y contraer obligaciones, administrar sus bienes y gestionar sus recursos, sujeto a las disposiciones que regulan la contratación pública y a la fiscalización de la Contraloría General de la República.

Que la ciberseguridad es un elemento fundamental para garantizar la protección de la información y los sistemas tecnológicos de los Estados, garantizando la seguridad de la información, la continuidad operativa de los servicios públicos y la confianza en la administración gubernamental.

Que la Autoridad Nacional para la Innovación Gubernamental (AIG), en su condición de rector de la tecnología en el Estado, debe garantizar la coordinación e implementación de mecanismos efectivos para la prevención y atención de incidentes cibernéticos.

Que mediante Decreto Ejecutivo No. 53 de 11 de junio de 2025 publicado en la Gaceta Oficial 30-298-A, se crea el Centro de Operaciones de Seguridad Gubernamental (SOC GUBERNAMENTAL), como una unidad operativa centralizada para la prevención, detección y respuesta ante incidentes de ciberseguridad con el propósito de salvaguardar la infraestructura digital del Estado, encargándose a la Autoridad Nacional para la Innovación Gubernamental para la administración y operación de esta.

Que el numeral 11 del artículo 3 de la Ley 65 de 2009, establece que para el cumplimiento de los objetivos de la Autoridad tendrá entre sus funciones la de emitir directrices para establecer los estándares necesarios para el desarrollo y la protección de los sistemas tecnológicos del Estado y velar por su cumplimiento, realizando inspecciones periódicas para identificar situaciones que requieran ser corregidas, por lo que se;

RESUELVE:

PRIMERO: ADOPTAR, los siguientes controles de Protección en Ciberseguridad para los Sistemas Informáticos en todas las entidades del Estado:

-Ámbito de Aplicación
La presente Resolución es de carácter obligatorio y de cumplimiento exigible para los Órganos Ejecutivo, Legislativo y Judicial del Estado, así como para las entidades autónomas, semiautónomas, descentralizadas y empresas estatales, así como sus dependencias, entidades adscritas y órganos auxiliares.

Para los Municipios, Juntas Comunales, Consejos Provinciales y Comarcales, sus disposiciones tendrán carácter de guía técnica de referencia, orientada a fortalecer las medidas mínimas de Ciberseguridad en sus sistemas informáticos.

-Medidas mínimas obligatorias de Protección en Ciberseguridad.

Las entidades comprendidas en el ámbito de aplicación obligatorio de la presente Resolución deberán garantizar que, previo a la puesta en producción y durante la operación de sus sistemas informáticos, se cumpla como mínimo con las siguientes medidas básicas de protección en ciberseguridad, aplicables a los activos tecnológicos:

1. Inventario de activos expuestos a Internet.

Mantener un inventario actualizado de los activos tecnológicos expuestos a Internet, incluyendo su finalidad, ubicación lógica y responsable designado.

2. Actualización y parchado de activos tecnológicos.

Mantener actualizados y con parches de seguridad aplicados todos los activos tecnológicos, incluyendo servidores, aplicaciones, servicios y dispositivos de red perimetral. Se le debe dar prioridad a aquellos activos que están expuestos a Internet.

3. Autenticación multifactor para accesos remotos

Implementar controles de autenticación multifactor (MFA), como mínimo, para:

a) el acceso remoto a la red institucional mediante VPN; y

b) el acceso a servicios de correo electrónico institucional desde fuera de la red interna de la entidad; y

c) plataformas en modalidad SaaS (Software as a Service), incluyendo redes sociales.

4. Sistemas operativos vigentes y con soporte.

Contar con sistemas operativos vigentes y con soporte del fabricante en la red interna y externa de la entidad.

En los casos en que no sea posible su actualización por razones técnicas u operativas debidamente justificadas, dichos equipos deberán mantenerse aislados de la red institucional y contar con medidas de mitigación adecuadas.

5. Protección contra malware.

La entidad deberá contar con soluciones de protección contra malware instaladas y activas en todas las estaciones de trabajo y servidores, manteniendo actualizadas las firmas o mecanismos de detección, de forma que permitan la identificación y mitigación de amenazas.

6. Segmentación perimetral mediante zona desmilitarizada (DMZ).

Los sistemas y servicios expuestos a Internet deberán ubicarse en una zona desmilitarizada (DMZ) o segmento de red perimetral equivalente y a su vez estar protegidos por un Web Application Firewall

En ningún caso los activos expuestos directamente a Internet podrán encontrarse alojados dentro de la red interna de la entidad sin los controles de segmentación correspondientes.

7. Restricción de accesos administrativos desde Internet.

Los accesos administrativos a sistemas expuestos a Internet, tales como SSH, RDP, SMB, accesos a bases de datos, interfaces de administración de dispositivos de red, entre otros, pero no limitados a estos, deberán estar restringidos, evitando su disponibilidad directa desde redes públicas y garantizando controles adicionales de acceso.

8. Prueba de penetración externa.

Realizar al menos una (1) prueba de penetración externa anual, cuyo alcance incluya los activos tecnológicos expuestos a Internet, documentando los hallazgos identificados y las acciones de remediación correspondientes.

9. Protección mediante filtrado de navegación web.

Contar con mecanismos de filtrado de navegación web, orientados a prevenir el acceso a sitios maliciosos, fraudulentos o de alto riesgo, incluyendo aquellos asociados a distribución de malware, phishing u otras amenazas cibernéticas. Dichos mecanismos deberán mantenerse operativos y actualizados.

10. Protección del correo electrónico institucional.

Contar con controles de seguridad para el correo electrónico institucional, orientados a detectar y bloquear correos maliciosos, incluyendo aquellos que contengan enlaces fraudulentos, archivos adjuntos peligrosos o intentos de suplantación de identidad. Estos controles deberán mantenerse activos y actualizados.

-Informe de Autogestión de Cumplimiento.

Las entidades para las cuales la presente Resolución tiene carácter obligatorio deberán remitir a la Autoridad Nacional para la Innovación Gubernamental (AIG), en un plazo no mayor a treinta (30) días calendario contados a partir de la entrada en vigencia de esta Resolución, un informe de autogestión sobre el nivel de cumplimiento de las medidas establecidas.

Cuando la entidad cumpla con un control, deberá adjuntar evidencia documentada que sustente su cumplimiento.

Cuando la entidad no cumpla con un control, deberá presentar un plan de acción, el cual deberá ejecutarse en un plazo máximo de cuarenta y cinco (45) días calendario, contados a partir del envío del informe de autogestión.

SEGUNDO: ORDENAR la publicación de la presente Resolución en la Gaceta Oficial de la República de Panamá

TERCERO: La presente Resolución comenzará a regir a partir de su publicación.

FUNDAMENTO DE DERECHO: Ley 65. De 30 de octubre de 2009. Que crea la Autoridad Nacional para la Innovación Gubernamental. G.O. 26400-C.

PUBLÍQUESE Y CÚMPLASE,

ADOLFO FÁBREGA
Administrador General

AUTORIDAD NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL
REPÚBLICA DE PANAMÁ

FRANCISCO GUINARD LINCE
Subadministrador General

ADOLFO PONS
Director Nacional de Ciberseguridad

AF/FG/AP/MAP/oa

GOBIERNO NACIONAL CON PASO FIRME | AIG AUTORIDAD NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL

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

Firma: _____

AIG ASESOR LEGAL