Lima, 22 de Octubre del 2025

RESOLUCION N° 000031-2025-AMAG/CD-P

VISTOS:

El Informe N° 000663-2025-AMAG/SA, de fecha 07 de octubre de 2025, de la Secretaría Administrativa, que sustenta la necesidad de designar al Oficial de Seguridad y Confianza Digital considerando la normativa vigente aplicable; el Informe N° 000469-2025-AMAG/OAJ, de fecha 17 de octubre de 2025, de la Oficina de Asesoría Jurídica que emite opinión legal favorable sobre el particular y el Informe N° 000184-2025-AMAG/DG, de fecha 21 de octubre de 2025, de la Dirección General.

CONSIDERANDO:

Que, el artículo 151° de la Constitución Política del Perú señala que la Academia de la Magistratura forma parte del Poder Judicial y se encarga de la formación y capacitación de jueces y fiscales en todos sus niveles, para los efectos de su selección, en concordancia con lo dispuesto en el artículo 2º de su Ley Orgánica, aprobada por Ley Nº 26335;

Que, la Ley N° 26335, Ley Orgánica de la Academia de la Magistratura, establece en su artículo 1° que la Academia de la Magistratura es una persona jurídica de derecho público interno que forma parte del Poder Judicial y que goza de autonomía administrativa, académica y económica, así como constituye un Pliego Presupuestal;

Que, mediante la Resolución N° 015-2022-AMAG-CD/P, de fecha 09 de marzo de 2022, se conformó el Comité de Gobierno Digital de la Academia de la Magistratura, así como se designó al Oficial de Seguridad;

Que, mediante Resolución N° 000030-2025-AMAG-CD/P, de fecha 22 de octubre de 2025, se dejó sin efecto la Resolución N° 015-2022-AMAG-CD/P, de fecha 09 de marzo de 2022 que conformó el Comité de Gobierno Digital y designó al Oficial de Seguridad;

Que, según la normativa vigente aplicable al Oficial de Seguridad y Confianza Digital, resulta necesario actualizar la designación de este;

Que, la Directiva Nº 001-2023-PCM/SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital, aprobada mediante Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD, publicada el 08 de setiembre de 2023, establece detalladamente el perfil en cuanto a conocimientos, formación y experiencia profesional que debe cumplir el que desempeña dicho rol, así como sobre su designación;

Que, el Subdirector de Informática mediante Informe N° 000209-2024-D-AMAG/SA-INF, de fecha 27 de diciembre de 2024, señala que no reúne requisitos de capacitación exigidos al perfil que debe desempeñar dicho rol;

Que, corresponde otorgar un plazo de seis (6) meses a la Subdirección de Recursos, para asegurar que el Oficial de Seguridad y Confianza Digital fortalezca sus conocimientos y formación profesional, a fin de cumplir con el perfil establecido en el literal b) del sub numeral

5.1.2 del artículo 5° de la Directiva Nº 001-2023-PCM/SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital; en concordancia con los establecido en el literal b) del sub numeral 8.4 de su artículo 8°;

En uso de las facultades conferidas por la Ley N° 26335 – Ley Orgánica de la Academia de la Magistratura; así como lo señalado en el Estatuto y el Reglamento de Organización y Funciones, ambos actualizados mediante Resolución N° 23-2017-AMAG-CD, de conformidad con el mandato legal y en ejercicios de las atribuciones conferidas.

SE RESUELVE:

ARTÍCULO PRIMERO. – DESIGNAR como Oficial de Seguridad y Confianza Digital a la Subdirección de Informática.

ARTÍCULO SEGUNDO. – ASIGNAR al Oficial de Seguridad y Confianza Digital, las siguientes responsabilidades y las demás que de acuerdo a la normativa aplicable le competen al desempeño de dicho rol:

a) Coordinar la implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad, atendiendo las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
b) Coordinar con las unidades de organización de la entidad las acciones orientadas a implementar y/o mantener el SGSI, de acuerdo con lo establecido por la alta dirección y las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
c) Formular y proponer políticas, procedimientos y planes en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad y confianza digital.
d) Promover la conformación y adecuada operación del equipo de respuestas ante incidentes de seguridad de la información.
e) Proponer medidas para la gestión de riesgos e incidentes de seguridad de la información, seguridad digital y ciberseguridad.
f) Crear y mantener un registro de los eventos e incidentes de seguridad de la información identificados.
g) Comunicar al Centro Nacional de Seguridad Digital (CNSD) los incidentes de seguridad digital críticos que afecten a los procesos misionales o servicios que brinda la entidad, y de ser el caso, coordinar y/o participar en su atención con el CNSD.
h) Planificar y coordinar la ejecución de pruebas de evaluación de vulnerabilidades de los aplicativos informáticos, sistemas, infraestructura, datos y redes que soportan los servicios digitales, procesos misionales o relevantes de la entidad.
i) Elaborar informes de los riesgos e incidentes de seguridad de la información críticos para la entidad pública e informarlos a la máxima autoridad administrativa.
j) Informar a la máxima autoridad administrativa acerca de los riesgos de seguridad de la información, incidentes de seguridad de la información críticos, avances y dificultades en la implementación u operación del SGSI, resultados de las auditorías de seguridad de la información internas y/o externas realizadas anualmente a la entidad, y sobre la aplicación efectiva de las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.

k) Coordinar con el CNSD acciones de sensibilización y capacitación para los funcionarios y servidores civiles de la entidad sobre seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
l) Coordinar con el Oficial de Gobierno de Datos y el Oficial de Datos Personales en todas las cuestiones relativas a la implementación de controles de seguridad de la información relacionados con las materias de gestión de datos y protección de datos personales en la entidad, respectivamente.
m) Coordinar con el Líder de Gobierno y Transformación Digital, lo concerniente a iniciativas y proyectos en materia de seguridad y confianza digital.
n) Coordinar con los dueños de procesos, propietarios de riesgos y responsables de las unidades de organización de la entidad su apoyo en la gestión de riesgos e implementación de los controles de seguridad de la información identificados en sus ámbitos de competencia, así como en la gestión de incidentes de seguridad de la información.
o) Liderar a los Coordinador de Seguridad y Confianza Digital (CSCD) designados en la entidad pública para la adecuada implementación del SGSI.
p) Asegurar y supervisar la adopción y uso de estándares, normas técnicas y mejores prácticas de seguridad de la información ampliamente reconocidos por parte de la unidad de organización de tecnologías de la información cuando ésta adquiera, tercerice o desarrolle software o implemente otro tipo de soluciones tecnológicas.
q) Coordinar con la unidad de organización responsable de las tecnologías de la información o la que haga sus veces en la entidad, cuando corresponda, en los temas relativos a sus responsabilidades.
r) Otras responsabilidades afines que le sean asignadas por el titular de la entidad o la máxima autoridad administrativa.

ARTÍCULO TERCERO. – OTORGAR un plazo de seis (06) meses a la Subdirección de Recursos, para asegurar que el Oficial de Seguridad y Confianza Digital fortalezca sus conocimientos y formación profesional, a fin de cumplir con el perfil establecido en el literal b) del sub numeral 5.1.2 del artículo 5 de la Directiva Nº 001-2023-PCM/SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital.

ARTÍCULO CUARTO. – DISPONER que la Dirección General notifique la presente Resolución al Oficial de Seguridad y Confianza Digital, para los fines pertinentes.

ARTÍCULO QUINTO. – DISPONER la publicación de la presente Resolución en el Portal Institucional de la Academia de la Magistratura (www.amag.edu.pe).

REGÍSTRESE, COMUNÍQUESE CÚMPLESE Y ARCHÍVESE.

Firmado digital

VICTOR HUGO CHANDUVI CORNEJO
PRESIDENTE DE CONSEJO DIRECTIVO
Academia de la Magistratura

VHCC/mmmm