

RESOLUCIÓN DE GERENCIA GENERAL

N° 108-2024-ADINELSA

ACTUALIZACIÓN DEL RESPONSABLE DEL ROL DE OFICIAL DE SEGURIDAD Y CONFIANZA DIGITAL DE ADINELSA

San Juan de Miraflores, 27 de noviembre de 2024

VISTOS:

El Informe N° 00175-2024-SGPC-ADINELSA de la Subgerencia de Planeamiento y Control de Gestión y;

CONSIDERANDO:

Que, con fecha 26 de marzo del 2019, la Corporación FONAFE mediante Oficio SIED N° 002-2019/OGR/FONAFE, indicó que era necesario se efectúe la conformación del Comité de Gobierno Digital;

Que, con fecha 04 de abril del 2019 mediante Resolución de Gerencia General N° 030-2019-ADINELSA, se conformó el Comité de Gobierno Digital de ADINELSA, el cual estuvo presidido por el Gerente General, teniendo como integrantes al Gerente de Administración y Finanzas, al Jefe del Departamento de Tecnología de la Información, al Jefe de la Oficina de Asesoría Legal y al Jefe del Departamento de Planeamiento y Control de Gestión;

Que, con fecha 01 de julio del 2020 mediante Resolución de Gerencia General N° 045-2020-ADINELSA se realizó la designación del Líder de Gobierno Digital en ADINELSA, el cual estuvo representado por el Gerente de Administración y Finanzas;

Que, con fecha 03 de marzo del 2021 se modificó la Resolución de Gerencia General N° 030-2019-ADINELSA en el punto segundo de la parte resolutive, reconvirmando el Comité de Gobierno Digital;

Que, con fecha 06 de septiembre del 2023, la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD, aprobó la Directiva N° 001-2023-PCM/SGTD denominada "Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital;

Firmas de aprobación:

Que, con fecha de 06 de junio del 2024, a través de la Resolución de Gerencia General N° 102-2024-SGPC-ADINELSA, se informó que la Oficina de Tecnologías de la Información y Comunicaciones asumiría la gestión del Sistema de Seguridad de la Información en ADINELSA, conforme a la norma ISO 27001;

Que, con fecha de 28 de junio del 2024, mediante Resolución de Gerencia General N° 115-2024-SGPC-ADINELSA, se formalizó la transferencia de la administración del servicio de gestión y coordinación de seguridad digital, bajo la norma ISO 27001, a la Oficina de Tecnologías de la Información y Comunicaciones desde el 01 de julio de 2024;

Que, con Informe N° 00175-2024-SGPC-ADINELSA de fecha 05 de noviembre de 2024 la Subgerencia de Planeamiento y Control de Gestión señala que, de acuerdo con la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD y la Directiva N° 001-2023-PCM/SGTD, que establece el Perfil y las Responsabilidades del Oficial de Seguridad y Confianza Digital resulta necesario designar a la persona como Oficial de Seguridad y Confianza Digital (OSCD), asumiendo este rol la Jefatura de la Oficina de Tecnologías de la Información y Comunicaciones, ya que el artículo 111 del Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, aprobado mediante Decreto Supremo N° 029-2021-PCM dispone que el Oficial de Seguridad Digital (actualmente, Oficial de Seguridad y Confianza Digital) es el rol responsable de coordinar la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en la entidad, atendiendo las normas en materia de seguridad digital, confianza digital y gobierno digital."

Que, el citado Informe N° 00175-2024-SGPC-GG-ADINELSA indica que la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD y la Directiva N° 001-2023-PCM/SGTD establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital y se aplica a las empresas públicas de los gobiernos regionales y locales, y las que se encuentren en el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE); señalándose en los numerales 3.1. y 3.2. del artículo 3 de la Directiva lo siguiente:

3.1 El Oficial de Seguridad y Confianza Digital es el rol responsable de coordinar la implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) en la entidad pública. Dicho rol recae en un funcionario o servidor civil, de la entidad pública que cuente con el conocimiento experiencia profesional y formación, de acuerdo con lo establecido en la Directiva.

Firmas de aprobación:

3.2 El Oficial de Seguridad y Confianza Digital es un rol estratégico para la gestión digital en la entidad pública, reporta y depende de la máxima autoridad administrativa, y actúa de conformidad con lo establecido en el marco legal de seguridad y confianza digital.

Que, asimismo el Informe N° 00175-2024-SGPC-GG-ADINELSA indica que la Directiva N° 001-2023-PCM/SGTD denominada "Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital", establece que el Oficial de Seguridad y Confianza Digital tiene como responsabilidades:

- a) Coordinar la implementación, operación, mantenimiento y mejora continua del 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 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.

Firmas de aprobación:

- 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 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.

Firmas de aprobación:

r) Otras responsabilidades afines que le sean asignadas por el titular de la entidad o la máxima autoridad administrativa.

Que, el mencionado Informe N° 00175-2024-SGPC-GG-ADINELSA concluye que con la designación del nuevo del Oficial de Seguridad y Confianza Digital se llevará a cabo la implementación, operación, mantenimiento y mejora continua del SGSI, además de apoyar en priorización e implementación de procesos para la transformación digital, en coordinación con las distintas áreas, unidades orgánicas, programas o proyectos de la entidad, señalando además que, las responsabilidades del Oficial de Seguridad y Confianza Digital se reflejarán en el Manual de Roles y Responsabilidades del Sistema de Seguridad de la Información.

Que, en ese contexto y en virtud de la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD, la Directiva N° 001-2023-PCM/SGTD que establece el Perfil y las Responsabilidades del Oficial de Seguridad y Confianza Digital y el Informe N° 00175-2024-SGPC-GG-ADINELSA resulta necesario proceder con la actualización del responsable del rol de Oficial de Seguridad y Confianza Digital (OSCD) de ADINELSA.

Estando a lo manifestado en las consideraciones precedentes, y con la conformidad de la Gerencia General;

SE RESUELVE:

PRIMERO. – Actualizar al responsable del rol de Oficial de Seguridad y Confianza Digital (OSCD) de ADINELSA, cuya función será asumida por la Jefatura de la Oficina de Tecnologías de la Información y Comunicaciones.

SEGUNDO. – Disponer que el Oficial de Seguridad y Confianza Digital (OSCD) cumpla con las siguientes responsabilidades:

a) Coordinar la implementación, operación, mantenimiento y mejora continua del 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.

Firmas de aprobación:

- 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 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.

Firmas de aprobación:

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 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.

TERCERO. – Disponer que la Oficina de Trámite Documentario notifique la presente resolución al Jefe de la Oficina de Tecnologías de la Información y Comunicaciones, para los fines correspondientes.

CUARTO. – Dejar sin efecto la Resolución de Gerencia General N° 100-2023- ADINELSA de fecha 05 de diciembre de 2023.

QUINTO. – Encargar a la Subgerencia de Planeamiento y Control de Gestión la comunicación de la presente Resolución a la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros y su respectivo registro en la web <https://facilita.gob.pe/t/42>.

SEXTO. – Disponer la publicación de la presente Resolución en el Portal Institucional de Empresa de Administración de Infraestructura Eléctrica S.A. - ADINELSA (www.adinelsa.com.pe), en el plazo máximo de dos (02) días hábiles contados desde su emisión.

Regístrese, comuníquese y publíquese.

Wilber Suárez Vargas
Gerente General

Firmas de aprobación:



Esta es una copia auténtica imprimible de un documento electrónico archivado por ADINELSA, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la lectura del código QR o el siguiente enlace:
<https://tramite.adinelsa.com.pe/consulta/dlFile?var=t8GFuYOAflWzqL%2FAj2%2FNhmOjZVldoJJlqF14d17gw9Y%3D>