"AÑO INTERNACIONAL DE LA CONSERVACIÓN DE LOS GLACIARES"
"2018 - 2027 DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
"AÑO DE LA RECUPERACIÓN Y CONSOLIDACIÓN DE LA ECONOMÍA PERUANA"

MUNICIPALIDAD PROVINCIAL MARISCAL NIETO

LEY ORGÁNICA N° 27972 DEL 26-05-2003
LEY N° 8230 DEL 03-04-1936

RESOLUCIÓN DE ALCALDÍA N.° 00297 -2025-A/MPMN

Moquegua, 29 AGO. 2025

VISTOS: La Carta N. 002-2025-LGTD-ECC/MPMN, Informe N° 0356-2025-OTIE/GM/MPMN, e Informe Legal N° 1049-2025/GAJ/GM/MPMN, y;

CONSIDERANDO:

Que, de conformidad a lo establecido en el Artículo 194° de la Constitución Política del Estado, modificado por la Ley de Reforma de la Constitución Política del Perú - Ley N° 30305, en concordancia con el Artículo II del Título Preliminar de la Ley N° 27972 - Ley Orgánica de Municipalidades, se establece que, los Gobiernos Locales gozan de autonomía política, económica y administrativa en los asuntos de su competencia;

Que, conforme a la Ley Orgánica de Municipalidades Ley N° 27972, señala que los Gobiernos Locales promueven el desarrollo integral para viabilizar el crecimiento económico, la justicia social y la sostenibilidad ambiental, siendo que la promoción del desarrollo local se realiza en coordinación y asociación con los niveles de Gobierno Regional y Nacional, con el objetivo de facilitar la competitividad local y propiciar las mejoras condiciones de vida de su población;

Que, conforme a lo dispuesto en el numeral 6 del artículo 20 concordante con el artículo 43 de la Ley Orgánica de Municipalidades, señalan como una de las atribuciones del alcalde, dictar Resoluciones de Alcaldía y por las cuales aprueba y resuelve, los asuntos de carácter administrativo;

Que, el artículo 8 del Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital, **tiene por objeto** establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la administración pública en los tres niveles de gobierno.

Que, el artículo 6 del precitado Decreto Legislativo, **define al Gobierno Digital** como el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público; y, comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza gestión de implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos.

Que, asimismo, el artículo 30 del precitado Decreto Legislativo **define la Seguridad Digital** como el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

Que, de acuerdo con el precitado artículo, la Ley de Gobierno Digital **crea** en su artículo 31 **el Marco de Seguridad Digital del Estado Peruano**, el cual se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública.

Que, la nota 1 del artículo 2 del Decreto Supremo N° 050-2018-PCM, que aprueba la definición de seguridad digital en el ámbito nacional, señala que la confianza en el entorno digital o también denominada confianza digital emerge como resultado de cuán veraz, predecible, seguro y confiable son las interacciones digitales que se generan entre empresas, individuos o cosas.

Que, el Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento, **tiene por objeto** establecer las medidas que resultan necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional.

Que, el articulo 9 en el numeral 9.3 del precitado decreto, establece que las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la información (SGSI), un Equipo de Respuestas ante Incidentes de Seguridad Digital cuando corresponda y cumplir con la regulación emitida por la Secretaría de Gobierno Digital.

Que, ante los riesgos en el entorno digital o ciberataques se hace necesario e indispensable que las entidades de la administración pública establezcan mecanismos y espacios de coordinación técnica y especializada para gestionar todo incidente de seguridad digital que afecte sus procedimientos, procesos y servicios, procurando fortalecer la confianza digital de las personas y ciudadanos.

Que, mediante el Decreto Supremo N° 029-2021-PCM, se aprueba el Reglamento del Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.

Que, el artículo 104 de la norma antes acotada, **define al Equipo de Respuestas** ante Incidentes de Seguridad Digital como aquel equipo responsable de la gestión de incidentes de seguridad digital que afectan los activos de una entidad pública o una red de confianza. Su implementación y conformación se realiza en base a las disposiciones que determine la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros.

Que, asimismo, el articulo precitado indica que **las entidades** de la Administración pública **conforman** un Equipo de Respuestas ante Incidentes de Seguridad Digital de carácter institucional. Dichos Equipos forman parte de los órganos o unidades orgánicas de Tecnologías de la Información de la entidad o de la unidad de organización especializada en seguridad de la información o similar prevista en su estructura orgánica o funcional. Su conformación es comunicada a la Secretaría de Gobierno Digital mediante los mecanismos dispuestos para tal fin.

Que, de igual modo, dicho artículo indica que la Secretaría de Gobierno Digital, en su calidad de ente rector de la seguridad digital en el país, emite opinión técnica especializada a pedido de una entidad a fin de revisar o validar aspectos técnicos sobre la conformación de un Equipo de Respuesta ante incidentes de Seguridad Digital.

Que, el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros ha emitido la "Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital", para orientar a las entidades públicas en la conformación e implementación Equipo de Respuestas ante Incidentes de Seguridad Digital y se constituye como un documento de trabajo referencial para dicha conformación; estableciendo en el numeral 2.9 que el citado equipo es el responsable de la gestión de incidentes de seguridad digital que afectan los activos de una entidad pública o una red de confianza, conformado principalmente por especialistas en seguridad de las tecnologías de la información o informática.

Que, el numeral 4.1.4 de la Guía en mención señala que el equipo de respuestas ante incidentes de seguridad digital es un equipo técnico conformado principalmente por especialistas en seguridad de las tecnologías de la información e informática, en tal sentido es responsabilidad de la citada área o la que haga sus veces, la determinación de las responsabilidades del CSIRT (Acrónimo de Computer Security Incidente Response Team) mediante la designación de los roles relevantes.

Que, mediante Carta N. 002-2025-LGTD-ECC/MPMN, de fecha 21 de julio 2025, el Ing. Edwin Coayla Cuayla, informa la necesidad de conformar un Equipo de Respuestas ante Incidentes de Seguridad Digital de la Municipalidad Provincial de Mariscal Nieto, asimismo menciona que el 09 del presente mes se ha sostenido una reunión virtual con el analista de Infraestructura CNSD-SGTD-PCM, para verificar el cumplimiento de la Meta "12 Implementación del Sistema de Gestión de Seguridad de la Información en cumplimiento del Decreto Supremo N.° 029-2021-PCM". Del cual señala también que, el Centro Nacional de Seguridad Digital de la Presidencia del Consejo de Ministros ha emitido la "Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital", para orientar a las entidades públicas en la conformación e implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital y se constituye como un documento de trabajo referencial para dicha conformación.

Que, del mismo documento del párrafo ut supra, señala que el CSIRT de la Municipalidad Provincial de Mariscal Nieto, es un equipo estratégico y técnico, conformado por gestores y especialistas en seguridad de las tecnologías de la información o informática , y es responsable de la gestión de incidentes de seguridad digital que afecte los activos de nuestra entidad municipal o una red de confianza, asimismo señala que el CSIRT de la Municipalidad Provincial de Mariscal Nieto, es responsable de gestionar la respuesta y/o

recuperación ante incidentes de seguridad digital que afecte a nuestra entidad Municipal y; coordinar y articular acciones con la Secretaría de Gobierno y Transformación Digital a través del Centro Nacional de Seguridad Digital, para atender los incidentes de seguridad digital. Por lo que menciona que el equipo de respuestas ante Incidentes de Seguridad Digital de nuestra entidad Municipal debe cumplir con las siguientes funciones:

a) Comunicar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.
b) Adoptar medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la entidad.
c) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de seguridad digital en su entidad.
d) Asegurar acciones de investigación y cooperación efectiva, eficiente y segura con el Centro Nacional de Seguridad Digital.
e) Proveer los recursos y medidas necesarias para asegurar la efectiva gestión de incidentes se seguridad digital.
f) Requerir a los proveedores de desarrollo de software el cumplimiento de estándares, normas técnicas y mejores prácticas de seguridad ampliamente reconocidos.
g) Coordinar y colaborar a través del Centro Nacional de Seguridad Digital con otros Equipos de Respuestas ante Incidentes de Seguridad Digital, con la finalidad de fortalecer la seguridad digital en el ámbito de las redes de confianza.

En función a ello mediante el documento citado en el 2.17 del presente informe, propone que el equipo de Respuestas ante Incidentes de Seguridad Digital sea conformado de la siguiente manera, cumpliendo los siguientes roles dentro del CSIRT:

N°	INTEGRANTES	ROL DEL CSIRT
1	Jefe de la Oficina de Tecnología de Información y Estadística	Coordinador del CSIRT
2	Analista de Sistemas PAD III	Gestor de Incidentes del CSIRT
3	Especialista	Gestor de Redes y Comunicaciones y Gestor de Infraestructura Digital

Que, mediante Informe N° 0356-2025-OTIE/GM/MPMN, de fecha 11 de agosto de 2025, el jefe de la Oficina de Tecnología de la Información y Estadística, Ing. Carlos Javier Perales Oviedo, solicita a la Gerencia Municipal, la conformación del Equipo de Respuestas ante Incidentes de Seguridad Digital, conforme a la propuesta señalada en la Carta N. 002-2025-LGTD-ECC/MPMN.

Que, mediante Informe Legal N° 1049-2025/GAJ/GM/MPMN, el Gerente de Asesoría Jurídica luego del análisis realizado a los documentos concluye que, es **PROCEDENTE,** que mediante resolución de alcaldía se realice la conformación del Equipo de Respuestas ante Incidentes de Seguridad Digital de la Municipalidad Provincial de Mariscal Nieto (...)"

Que, de conformidad con los considerandos expuestos, y, en ejercicio de las atribuciones y facultades conferidas por la Ley N° 27972, Ley Orgánica de Municipalidades, y estando a las visaciones correspondientes;

SE RESUELVE:

ARTÍCULO PRIMERO. – CONFORMAR, el Equipo de Respuestas ante Incidentes de Seguridad Digital de la Municipalidad Provincial de Mariscal Nieto, el cual estará integrado de la siguiente manera:

N°	INTEGRANTES	ROL DEL CSIRT
1	Jefe de la Oficina de Tecnología de Información y Estadística	Coordinador del CSIRT
2	Analista de Sistemas PAD III	Gestor de Incidentes del CSIRT
3	Especialista	Gestor de Redes y Comunicaciones y Gestor de Infraestructura Digital

ARTÍCULO SEGUNDO. – El Equipo de Respuestas ante Incidentes de Seguridad Digital de la Municipalidad Provincial Mariscal Nieto, tendrá las siguientes funciones:

a) Comunicar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.
b) Adoptar medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la entidad.
c) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de seguridad digital en su entidad.
d) Asegurar acciones de investigación y cooperación efectiva, eficiente y segura con el Centro Nacional de Seguridad Digital.
e) Proveer los recursos y medidas necesarias para asegurar la efectiva gestión de incidentes se seguridad digital.
f) Requerir a los proveedores de desarrollo de software el cumplimiento de estándares, normas técnicas y mejores prácticas de seguridad ampliamente reconocidos.
g) Coordinar y colaborar a través del Centro Nacional de Seguridad Digital con otros Equipos de Respuestas ante Incidentes de Seguridad Digital, con la finalidad de fortalecer la seguridad digital en el ámbito de las redes de confianza.

ARTICULO TERCERO. - **DEJAR SIN EFECTO,** todo acto administrativo que se oponga a la presente resolución.

ARTÍCULO CUARTO. - **ENCARGAR,** a Gerencia Municipal y a la Oficina de Tecnología de Información y Estadística el fiel cumplimiento del presente acto resolutivo y a Secretaría General la notificación a los integrantes del Equipo de Respuestas ante Incidentes de Seguridad Digital de la Municipalidad Provincial Mariscal Nieto y demás áreas pertinentes, para su conocimiento y acciones correspondientes.

ARTÍCULO QUINTO. - **ENCARGAR,** a la Oficina de Tecnología de la Información y Estadística, la publicación de la presente Resolución en el Portal Institucional de la Municipalidad Provincial Mariscal Nieto - Moquegua.

REGÍSTRESE, COMUNÍQUESE, CÚMPLASE Y ARCHÍVESE.

Municipalidad Provincial Mariscal Nieto

CPC. JOHN LARRY COAYLA
ALCALDE