Municipalidad Distrital de Characato

Resolución de Alcaldía
N° 152-2025-MDCH

Arequipa, 16 de setiembre del 2025

VISTO:

El Expediente Administrativo N° 00004486 - I/2025: Informe Técnico N° 0006-NORIE del Consultor Iván Alejandro Noriega Llerena; Memorándum N° 00473-2025-GM-MDCH de la Gerencia Municipal; Memorándum N° 00081-2025-OAF/MDCH de la Oficina de Administración Financiera; Informe N° 00067-2025-UI-MDCH del (E) de la Unidad de Informática; Informe N° 00123-2025-OAF/MDCH de la Oficina de Administración Financiera; Carta N° 0005-2025-NORIE del Consultor Iván Alejandro Noriega Llerena; Memorándum N° 00572-2025-GM-MDCH de la Gerencia Municipal; Memorándum N° 00089-2025-OAF/MDCH de la Oficina de Administración Financiera; Memorándum N° 00822-2025-GM-MDCH de la Gerencia Municipal; Memorándum N° 00112-2025-OAF/MDCH de la Oficina de Administración Financiera; Informe N° 00116-2025-UI-MDCH del (E) de la Unidad de Informática; Informe N° 00155-2025-OAF/MDCH; Carta N° 0212-2025-MMC-MDCH e Informe N° 0212-2025-MDCH-ALE del Asesor Legal Externo en Materia Administrativa; Informe N° 00220-2025-GM-MDCH de la Gerencia Municipal; Proveído N° 00615-2025-AL/MDCH del Despacho de Alcaldía y;

CONSIDERANDO:

Que, conforme a lo establecido en el artículo 194° de la Constitución Política del Perú, las municipalidades gozan de autonomía política, económica y administrativa en los asuntos de su competencia; la que según el artículo II del Título Preliminar de la Ley N° 27972, Ley Orgánica de Municipalidades, radica en la facultad de ejercer actos de gobierno, administrativos y de administración, con sujeción al ordenamiento jurídico;

Que, mediante Informe N° 00116-2025-UI-MDCH, el encargado de la Unidad de Informática procedió a realizar las evaluaciones técnicas respectivas, exponiendo lo pertinente a la gestión de seguridad, su necesidad de implementación, los principios rectores, concluyendo con su aprobación a la propuesta del sistema de gestión de seguridad de la información presentada por el consultor externo.

Que, el artículo 109 del Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, 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 Sistema de Gestión de Seguridad de la Información (SGSI) comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren. Asimismo, contempla la gestión de riesgos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de ciberseguridad y acciones de colaboración y cooperación. Que, el artículo 105 de la precitada norma, dispone que las entidades públicas tienen como una de sus obligaciones en seguridad digital, el implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).

Que, mediante RESOLUCIÓN DE SECRETARÍA DE GOBIERNO Y TRANSFORMACIÓN DIGITAL N° 003-2023-PCM/SGTD se procedió a ESTABLECER LA IMPLEMENTACIÓN Y MANTENIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, teniendo alcance dicha normativa sobre las entidades de la Administración Pública establecidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004- 2019-JUS, con excepción de las personas jurídicas señaladas en el numeral 8 del citado artículo.

Que, si bien dicha resolución establecía diversos aspectos a merituar, el Artículo 7 expone lo siguiente: *"Los proyectos especiales del Poder Ejecutivo y los gobiernos locales tipo B, D, E, F y G, conforme a la clasificación realizada por el Ministerio de Economía y Finanzas, en el marco del Programa de Incentivos a la Mejora de la Gestión Municipal, pueden implementar su SGSI atendiendo su contexto, tamaño, complejidad y estructura, no estando obligadas a formular un Plan SGSI, ni conformar un equipo de trabajo técnico para el SGSI. Sin perjuicio de lo indicado deben coordinar con el Centro Nacional de Seguridad Digital la implementación de medidas y controles de seguridad de la información para fortalecer la confianza digital en sus procesos y servicios".*
Que, en relación a dicha clasificación, la municipalidad distrital de Characato sería un tipo D, por lo que le aplica las salvedades normativas expuestas.

Que el Inciso 6 del Art. 20 de la Ley 27972, señala: "(...) 6. Dictar decretos y resoluciones de alcaldía, con sujeción a las leyes y ordenanzas"; por tanto, corresponde aprobar mediante Resolución de Alcaldía la implementación de medidas y controles del sistema de gestión.

Que, mediante Memorándum N° 00473-2025-GM-MDCH, Gerencia Municipal remite con carácter de urgente la Propuesta de Sistema de Gestión de Seguridad de la Municipalidad Distrital de Characato, alcanzada mediante Informe Técnico N° 0006-2025-NORIE, de fecha 30 de mayo de 2025, por el consultor Iván Alejandro Noriega Llerena, quien procede a indicar la necesidad y procedimiento de implementación de un sistema de gestión de seguridad de la información, asegurando que la Municipalidad cumpla con las obligaciones legales de protección de datos y seguridad digital, fortalezca su capacidad para gestionar riesgos de información que garantice la confianza ciudadana en los servicios electrónicos; el cumplimiento riguroso, desde el nombramiento del responsable hasta la implementación del SGSI, permitirá una gestión sostenible y alineada a la transformación digita del Estado.

Municipalidad Distrital de Characato

Resolución de Alcaldía
N° 152-2025-MDCH

Que, mediante Informe N°00067-2025-UI-MDCH, de fecha 13 de junio de 2025, en atención al Memorándum N° 00081-2025-OAF/MDCH, el encargado de la Unidad de Informática, hace llegar observaciones al documento propuesto por el consultor, debido a que este carece de normativa vigente, así como no cuenta con un plan de acción para la implementación como Sistema de Gestión; lo cual es informado a la Gerencia Municipal con Informe N° 00123-2025-OAF/MDCH.

Que, mediante Memorándum N° 00572 y N° 00822-2025-GM-MDCH, Gerencia Municipal requiere el levantamiento de observaciones respectivo, para cuyo efecto remite la Carta N° 005-2025-NORIE de fecha 19 de junio de 2025, por el cual, el consultor Iván Alejandro Noriega Llerena, procedió a remitir la nueva versión de propuesta de Sistema de Gestión de Seguridad de la Información, con el respectivo levantamiento de observaciones.

Que, mediante Informe N°00116-2025-UI-MDCH, de fecha 28 de agosto de 2025, en atención al Memorándum N° 00089 y N° 00112-2025-OAF/MDCH, el Ing. Marcos Renzo Bustamante Valencia en su calidad de encargado de la Unidad de Informática, precisa que la seguridad se define como el conjunto de políticas, procesos, controles, herramientas y roles destinados a proteger los activos de información de una organización, que se sustenta en los principios de confidencialidad, disponibilidad, trazabilidad y razonabilidad; en tal sentido, señala que, a pesar que el Palacio cuenta con un Sistema de Seguridad Perimetral (SHOPOS) y la protección de un antivirus, las entidades públicas enfrentan amenazas cibernéticas que ponen en riesgo la continuidad de los servicios digitales y la confianza ciudadana, motivo por el cual la Municipalidad Distrital de Characato está iniciando la implementación del Sistema de Seguridad de la Información dentro del marco legal vigente, a fin de minimizar riesgos y asegurar la continuidad operativa; en tal sentido, concluye que:

- La estrategia digital es un instrumento clave para impulsar la transformación del Municipio mejorando los servicios públicos; un plan de estrategia digital bien estructurado contribuirá a un Municipio más transparente, eficiente, inclusivo y resiliente frente a los retos de la transformación digital consolidando la relación de confianza entre el Municipio y la ciudadanía.
- El marco legal vigente, liderado por la Secretaría de Gobierno y Transformación Digital, establece la obligatoriedad de implementar planes de estrategia digital con un enfoque integral y seguro.
- La aprobación del plan de estrategia digital permitirá reducir brechas tecnológicas, garantizar la seguridad digital, promover la innovación y facilitar la interoperabilidad en el sector público.
- Finalmente, vista y analizada la Propuesta del Plan de Estrategia Digital para la Municipalidad Distrital de Characato elaborada por el consultor Iván Alejandro Noriega Llerena, donde se indican y sustentan los Lineamientos establecidos por la Secretaría de Gobierno y Transformación Digital (SGTD) de la Presidencia del Consejo de Ministros en lo referido a la transformación digital para el sector público específicamente en lo que corresponde a la estrategia digital es que se APRUEBA la propuesta del Plan de Estrategia Digital presentada y se solicita remitirlo al Comité de Gobierno y Transformación Digital para su conocimiento y posterior aprobación por el titular de la entidad a través de una resolución u otro acto administrativo para luego informar a la Secretaría de Gobierno y Transformación Digital sobre el acto resolutivo en mención.

Que, mediante Informe N°00155-2025-OAF/MDCH, de fecha 28 de agosto de 2025, la Lic. Susana Dolores Torres Zegarra, Jefe de la Oficina de Administración Financiera refrenda el Informe N° 00116-2025-UI-MDCH emitido por el Encargado de la Unidad de Informática, emitiendo opinión favorable para la aprobación de la propuesta de Sistema de Gestión de Seguridad considerando viable la aprobación de la propuesta alcanzada, en atención a los fundamentos expuestos por la Unidad de Informática; la cual cuenta con opinión favorable del Asesor Legal Externo en Materia Administrativa, según Informe N° 0212-2025-MDCH-ALE

Que, mediante Proveído N° 00619-2025-AL-MDCH, el Despacho de Alcaldía dispone la emisión de Resolución de Alcaldía que aprueba la Implementación de medidas y controles de sistema de gestión de seguridad de la información, conforme lo solicita la Gerencia Municipal mediante informe N° 00229-2025-GM-MDCH.

Estando en las facultades otorgadas por el artículo 6° de la Ley Orgánica de Municipalidades - Ley N° 27972, por la Constitución Política del Perú y a la parte considerativa de la presente.

SE RESUELVE:

ARTÍCULO PRIMERO: APROBAR EL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION DE LA MUNICIPALIDAD DISTRITAL DE CHARACATO, la cual, como anexo forma parte integrante de la presente Resolución de Alcaldía.

ARTÍCULO SEGUNDO: ENCARGAR a la Unidad de Informática, la implementación del Sistema de Gestión de Seguridad de la Información, aprobado en el artículo precedente

ARTÍCULO TERCERO: DISPONER que la Unidad de Informática notifique el contenido del Sistema de Gestión de la Información a la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.

ARTÍCULO CUARTO: DISPONER a la Oficina de Informática la publicación de la presente Resolución de Alcaldía en el Portal Institucional de la Municipalidad Distrital de Characato (https://munichar acato.gob.pe) y en el Portal de Transparencia Estándar.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE

MUNICIPALIDAD DISTRITAL DE CHARACATO
Abog. Yadira Velazco Agramonte de Moscoso
Secretaria General

MUNICIPALIDAD DISTRITAL DE CHARACATO
Zerafin N. Pinto Pinto
ALCALDÍA

MUNICIPALIDAD DE CHARACATO

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Characato, Arequipa, Arequipa

Índice

1. Introducción

La Política del Sistema de Seguridad de la Información tiene como propósito implementar un conjunto de medidas orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información, los pilares fundamentales de la seguridad de la información. Su objetivo es definir los requisitos necesarios para proteger los datos, los equipos y los servicios tecnológicos que respaldan la mayoría de los procesos de la Municipalidad Distrital de Characato. Esta Política constituye el eje central que regula el Marco Normativo de Seguridad de la Información de la Municipalidad Distrital de Characato.

En un entorno donde las tecnologías de la información enfrentan amenazas en constante evolución, es esencial mantener un esfuerzo continuo para adaptarse y gestionar los riesgos asociados. Por su parte la Municipalidad Distrital de Characato reconoce que la información es un activo esencial para la institución y se compromete a preservar su integridad, confidencialidad y disponibilidad mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema permite gestionar los riesgos de los activos de información y, dentro del marco legal aplicable, fomenta la mejora continua del SGSI.

1.1. Objetivo

El propósito fundamental de esta Política de alto nivel es establecer los principios y las normas básicas para la gestión de la seguridad de la información. Su objetivo final es asegurar que la Municipalidad Distrital de Characato proteja la seguridad de la información y reduzca al mínimo los riesgos de naturaleza no financiera asociados a los impactos derivados de una gestión inadecuada.

1.2. Alcance

La Política abarca a toda la Municipalidad Distrital de Characato, tanto a todo trabajador público dentro y fuera de las sedes de la institución, así como a terceros colaboradores no relacionados directamente con la Municipalidad Distrital de Characato; estos deberán cumplir este mínimo requisito sin perjuicio de tener políticas más restrictivas y mejorar la seguridad en la medida de lo posible. El alcance de la presente Política abarca toda la información con independencia de la forma en la que se procese, quién acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente. La Política deberá estar disponible en la página web de la Municipalidad Distrital de Characato y en un repositorio común, de forma que sea accesible a todo el personal.

2. Marco legal

- **Ley N° 29733 – Ley de Protección de Datos Personales**: Establece la obligación de implementar medidas técnicas y organizativas de seguridad, acorde a estándares internacionales, para proteger los datos personales administrados por entidades públicas.
- **Decreto Supremo N° 003-2013-JUS**: Aprueba el Reglamento de la Ley N.° 29733, definiendo los requisitos mínimos del SGSI, basados en la ISO/IEC 27001:2022, para garantizar la confidencialidad, integridad y disponibilidad de la información.

- **Decreto Legislativo N° 1412 – Ley de Gobierno Digital** y **DS N° 029-2021-PCM** (Reglamento): Mandatan la adopción de plataformas y sistemas digitales seguros, así como la gobernanza y roles (incluido el Oficial de Seguridad Digital) necesarios para la transformación digital de las entidades públicas.
- **Decreto Supremo N° 050-2018-PCM**: Define la "Seguridad Digital" como componente de la Gestión de Tecnologías de la Información en el Estado, y establece lineamientos para su implementación en las entidades públicas.
- **Decreto de Urgencia N° 006-2020**: Crea el Sistema Nacional de Transformación Digital e impone a las entidades reportar sus avances en seguridad de la información en el Observatorio Nacional de Ciudadanía Digital.
- **Resolución de Secretaría de Gobierno Digital N° 005-2018-PCM/SEGDI**: Aprueba los lineamientos para la formulación del Plan de Gobierno Digital, que incluye la obligatoriedad de un SGSI alineado al Plan Estratégico Institucional y a la Política Nacional de Gobierno Electrónico.

3. Principios base de la Política de la Información

Esta Política se fundamenta en las mejores prácticas de Seguridad de la Información establecidas en el Estándar Internacional ISO/EC 27001 y asegura el cumplimiento de la legislación vigente en materia de protección de datos personales, así como de las normativas aplicables en el ámbito de la Seguridad de la Información que puedan impactar a la Municipalidad Distrital de Characato.

- **Alcance estratégico:** La seguridad de la información deberá contar con el compromiso y apoyo de todos los niveles directivos de la Municipalidad Distrital de Characato de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz.
- **Seguridad integral:** La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.
- **Gestión de riesgos:** El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.
- **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- **Mejora continua:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y

sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado.

- **Seguridad por defecto:** Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

La Municipalidad Distrital de Characato dispone que las funciones de Seguridad de la Información deberán quedar integradas en todos los niveles jerárquicos de su personal. Puesto que la Seguridad de la Información incumbe a todo el personal de la MDCH, esta Política deberá ser conocida, comprendida y asumida por todos sus funcionarios y colaboradores.

Para la consecución de los objetivos de esta Política, la MDCH deberá establecer una estrategia preventiva de análisis sobre los riesgos que pudieran afectarle, identificándolos, implantando controles para su mitigación y estableciendo procedimientos regulares para su revaluación.

4. Compromiso de la Alta Dirección

La Alta Dirección de la MDCH, consciente de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos institucionales, se compromete a:

- Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
- Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Impulsar la divulgación y la concienciación de la Política de Seguridad de la Información entre los colaboradores de la MDCH.
- Exigir el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- Considerar los riesgos de seguridad de la información en la toma de decisiones.

5. Roles y responsabilidades

La Municipalidad Distrital de Characato (MDCH) asume el compromiso de proteger la seguridad de todos los activos bajo su responsabilidad mediante la implementación de las medidas necesarias, asegurando en todo momento el cumplimiento de las normativas y leyes aplicables. Asimismo, la MDY designará una figura responsable de definir, implementar y supervisar las medidas de ciberseguridad y seguridad de la información. Esta figura, que operará desde un marco de gobierno y gestión, será independiente de cualquier área organizativa, reportando directamente al órgano de gobierno o, en su defecto, a la comisión de auditoría. Entre sus funciones y responsabilidades destacan la aplicación de principios de segregación de funciones y la comunicación con las autoridades y grupos de interés especializados en seguridad de la información.

6. Directivas

6.1. Directivas sobre medidas de seguridad de la información.

- La Unidad de Informática deberá informar de manera periódica a los usuarios acerca de las restricciones y controles de seguridad implantados en la institución, a fin de garantizar la protección de la información gestionada.
- Al menos una vez al año, la Unidad de Informática elaborará un inventario de los activos de información bajo su responsabilidad, detallando para cada uno: tipo de activo, estado operativo y responsable asignado, quien asumirá la custodia y el uso adecuado del mismo.
- La información procesada deberá respaldarse con una periodicidad acorde a su frecuencia de modificación, asegurando la disponibilidad de recuperables actualizados.
- Los datos almacenados se conservarán durante el periodo que la institución estime pertinente, en cumplimiento de la normativa vigente emitida por la autoridad competente.
- El Responsable de Seguridad de la Información supervisará y validará todas las actividades de respaldo de datos.

6.2. Directivas de carácter preventivo

- Se establecerán rutinas de auditoría de los registros de actividad de los sistemas para detectar de forma temprana acciones sospechosas, tanto internas como externas.
- Se documentará y respaldará periódicamente la configuración de los sistemas; además, se realizarán comparaciones entre la configuración operativa actual y la configuración base establecida.
- Los incidentes y vulnerabilidades de seguridad detectados en los sistemas de información deberán comunicarse de forma oportuna y efectiva para posibilitar la implementación de acciones correctivas inmediatas.
- El acceso de los usuarios a los recursos informáticos se limitará estrictamente a sus funciones y responsabilidades, bajo un modelo de privilegios mínimos.
- Todos los servicios y procedimientos administrativos ofrecidos a la ciudadanía deberán utilizar mecanismos de cifrado robusto para la transmisión y almacenamiento de datos.
- Se desplegará un sistema antivirus actualizado en la totalidad de los activos informáticos compatibles.
- Se dispondrá de dispositivos de almacenamiento (discos duros SCSI o SATA) adecuados para el respaldo periódico de la información.
- Se garantizará un suministro eléctrico confiable mediante tierra física, estabilizadores, sistemas UPS, grupos electrógenos y redes independientes de alimentación.

6.3. Directivas sobre recuperación de la información

- Se definirán procedimientos de contingencia que permitan minimizar el impacto de incidentes y salvaguardar la información de bases de datos, aplicaciones, sistemas operativos y comunicaciones.

- Dichos procedimientos deberán estar documentados y difundidos entre el personal de la Unidad de Informática.
- La Unidad de Informática desarrollará un plan de contingencia integral que incluya: identificación de riesgos, definición de soluciones, estrategias de recuperación, documentación de procesos, realización de pruebas periódicas, implementación y mejora continua.
- Se impartirán cursos de capacitación y se realizarán simulacros regulares para evaluar la capacidad de respuesta del personal en la recuperación de sistemas completos (sistema operativo, aplicaciones, servicios y datos).

6.4. Directivas sobre redes, servidores autogestionados y servicios tercerizados

- La red local y el sistema de conectividad a Internet deben contar con sistemas de seguridad.
- Se deberá contar con técnicas de seguridad que se evalúen como convenientes: Cortafuegos, detección de intrusos, inspección de contenido, auditoria, filtrado, Proxy, criptografía o autenticación; que permitan controlar la seguridad de los usuarios de la red local y del sistema de conectividad a Internet.
- Se implementarán políticas de asignación y restricción de direcciones IP basadas en roles y funciones de los usuarios.
- Se mantendrá actualizada y debidamente documentada la topología de la red (sedes, dispositivos, direcciones IP y demás elementos relevantes) para su supervisión y auditoría.
- Se considera falta grave que los usuarios eludan intencionalmente las configuraciones de bloqueo de software o sitios web establecidas por la entidad.
- Solo permanecerán habilitados los servicios de comunicación necesarios en los servidores; se minimizará el número de aplicaciones y puertos abiertos.
- Se deshabilitarán las cuentas de sistema de usuarios que hayan cesado sus labores o se encuentren en situación de licencia.
- Se implementarán procedimientos de validación continua de los servicios de datos y otros procesos, con el objetivo de garantizar una disponibilidad de 24×7.

6.5. Directivas relacionadas con la seguridad Física de los activos informáticos

- Los equipos de cómputo y almacenamiento recibirán mantenimiento preventivo y correctivo conforme a sus especificaciones técnicas o a un cronograma establecido.
- Se elaborarán y difundirán documentos normativos y guías de buenas prácticas para el uso y tratamiento de los equipos, con el fin de resguardar la seguridad física de los activos críticos de la Municipalidad.
- Las áreas de almacenamiento de medios de información mantendrán condiciones controladas de temperatura y humedad, entre otros parámetros ambientales.
- El acceso a dichas áreas estará restringido exclusivamente al personal autorizado, bajo la supervisión del Responsable de Seguridad de la Información.