REPÚBLICA DEL ECUADOR

Resolución Nro. SNAI-SNAI-2026-0052-R

Quito, D.M., 15 de mayo de 2026

SERVICIO NACIONAL DE ATENCIÓN INTEGRAL A PERSONAS ADULTAS PRIVADAS DE LA LIBERTAD Y A ADOLESCENTES

CONSIDERANDO:

Que, el artículo 226 de la Constitución de la República del Ecuador dispone que las instituciones del Estado, sus organismos, dependencias, servidoras y servidores públicos ejercerán únicamente las competencias y facultades que les sean atribuidas en la Constitución y la ley, y tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución;

Que, el artículo 227 de la Constitución de la República del Ecuador determina que la administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación;

Que, el Código Orgánico Administrativo establece el régimen jurídico aplicable al ejercicio de la función administrativa, así como los principios, competencias, formas de actuación, deber de motivación, coordinación administrativa, conservación de documentos y responsabilidad de las instituciones y servidores públicos;

Que, el Código Orgánico Integral Penal regula el Sistema Nacional de Rehabilitación Social, determina las competencias del Organismo Técnico y prevé la ejecución de penas, medidas, beneficios, regímenes y actuaciones relacionadas con el seguimiento de personas sometidas a control jurisdiccional;

Que, mediante Decreto Ejecutivo Nro. 366 se expidió el Reglamento del Sistema Nacional de Rehabilitación Social, el cual desarrolla disposiciones relacionadas con la instalación, activación, control, monitoreo, seguimiento, desactivación, desinstalación y retiro de dispositivos de vigilancia electrónica, así como con la información a la autoridad judicial, incidentes, requisitos de instalación y expedientes de usuarios;

Que, el Decreto Ejecutivo Nro. 366 regula el valor por uso y mantenimiento del dispositivo de vigilancia electrónica, los mecanismos de exoneración, reducción o diferimiento del pago, y la verificación del pago o de la resolución administrativa correspondiente como parte de los requisitos para la instalación del dispositivo;

Que, mediante resolución Nro. SNAI-SNAI-2026-0050-R de 14 de mayo de 2026 suscrito por Mgs. Mauricio Fernando Mayorga Vallejo Director General del SNAI, expide las Disposiciones Generales y Valor Por El Uso y Mantenimiento del Dispositivo de Vigilancia Electrónica.

Que, mediante memorando Nro. SNAI-SMCEPMS-2026-1178-M de 14 de mayo de 2026 suscrito por la Dra. Andrea Nicoole Camacho Guerrero Subdirectora de Medidas Cautelares, Ejecución de Penas y Medidas Socioeducativas que en su parte pertinente manifiesta: *"Al respecto, me permito solicitar a su autoridad que, autorice y disponga a la Dirección de Asesoría Jurídica, que realice la revisión del Informe Técnico Nro. SNAI-DPNPLDVER-IT-2026-0002 y la elaboración del Reglamento Técnico para la Gestión del Servicio de Vigilancia Electrónica y Uso de Dispositivos de Vigilancia Electrónica."*

Que, mediante informe tecnico Nro. SNAI-DPNPLDVER-IT-2026-0002 de 14 de mayo de 2026 suscrito por la señora Elionora Salazar Directora de Penas no Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción en sus recomendaciones manifiesta: *"5.1. Remitir el presente informe técnico y el proyecto de Resolución que contiene el Reglamento Técnico para la Gestión del Servicio de Vigilancia Electrónica y Uso de Dispositivos de Vigilancia Electrónica a la Dirección de Asesoría Jurídica, a fin de que se sirva revisar el instrumento y emitir el criterio jurídico correspondiente sobre su viabilidad, competencia de la autoridad emisora, técnica normativa y armonía con el ordenamiento jurídico vigente. 5.2. Solicitar a la Dirección de Asesoría Jurídica que, de considerarlo pertinente, emita observaciones, recomendaciones o ajustes al proyecto de Resolución y Reglamento Técnico, con la finalidad de fortalecer su contenido previo a su aprobación por la*

autoridad competente. 5.3. Continuar con el trámite administrativo correspondiente para la expedición del Reglamento Técnico, una vez que se cuente con la revisión jurídica respectiva y con las validaciones institucionales que correspondan. 5.4. Disponer que el proyecto de Reglamento Técnico sea socializado con las áreas técnicas, operativas, administrativas, financieras, jurídicas, tecnológicas y territoriales que intervienen en la gestión del Servicio de Vigilancia Electrónica, a fin de garantizar su correcta implementación y aplicación uniforme. 5.5. Recomendar que, una vez expedida la Resolución, la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción coordine la actualización de formatos, matrices, actas, informes, bitácoras y demás instrumentos necesarios para la aplicación del Reglamento Técnico. 5.6. Recomendar que se desarrollen procesos de capacitación o socialización dirigidos al personal técnico, operadores de monitoreo, supervisores, responsables territoriales y demás servidores intervinientes, con el objeto de asegurar el conocimiento y cumplimiento de las disposiciones contenidas en el Reglamento Técnico. 5.7. Recomendar que la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción mantenga mecanismos de seguimiento y mejora continua respecto de la aplicación del Reglamento Técnico, especialmente en materia de instalación, monitoreo, atención de alertas, soporte técnico, cambio o sustitución de dispositivos, gestión documental, reserva de la información y coordinación con autoridades competentes."

Que, mediante informe juridico Nro. SNAI-DAJ-IF-2026-0016 de 14 de mayo de 2026 suscrito por Abg. Raúl Andrade Director de Asesoría Jurídica en sus recomendaciones manifiesta: *"Emitir la Resolución correspondiente para la expedición del Reglamento Técnico para la Gestión del Servicio de Vigilancia Electrónica y Uso de Dispositivos de Vigilancia Electrónica, con la firma de la máxima autoridad del SNAI o del funcionario en quien se haya delegado expresamente la facultad normativa interna. • Verificar la compatibilidad de las disposiciones del Reglamento Técnico con la Ley Orgánica de Protección de Datos Personales y con la normativa sectorial aplicable en materia de seguridad de la información, previo a su aprobación definitiva. • Socializar el instrumento aprobado con las áreas técnicas, operativas, administrativas, financieras, jurídicas, tecnológicas y territoriales del SNAI que intervienen en la gestión del Servicio de Vigilancia Electrónica, a fin de garantizar su correcta aplicación. • Implementar procesos de capacitación dirigidos al personal técnico, operadores de monitoreo, supervisores y responsables territoriales, con el objeto de asegurar el conocimiento y cumplimiento uniforme de las disposiciones del Reglamento Técnico. • Establecer mecanismos de seguimiento, evaluación y mejora continua de la aplicación del Reglamento Técnico, en coordinación con la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción."*

Que, mediante sumilla inserta el señor Director General dirigida al Director de Asesoria Juridica manifiesta: *"Estimado Director, favor su análisis y trámite pertinente conforme normativa legal vigente."*

Que, resulta necesario contar con un instrumento técnico, administrativo y operativo que unifique los procedimientos internos para la gestión del Servicio de Vigilancia Electrónica y el uso de Dispositivos de Vigilancia Electrónica, garantizando trazabilidad, seguridad de la información, coordinación interinstitucional, control de calidad, mejora continua y cumplimiento oportuno de las disposiciones emitidas por autoridad judicial competente;

En ejercicio de las atribuciones y facultades que le confiere el Decreto Ejecutivo 626 de 13 de mayo de 2025 y el 366 de 22 de abril de 2026;

RESUELVE:

EXPEDIR EL REGLAMENTO TÉCNICO PARA LA GESTIÓN DEL SERVICIO DE VIGILANCIA ELECTRÓNICA Y USO DE DISPOSITIVOS DE VIGILANCIA ELECTRÓNICA

CAPÍTULO I

GENERALIDADES

Resolución Nro. SNAI-SNAI-2026-0052-R

Quito, D.M., 15 de mayo de 2026

Artículo 1.- Objeto. Establecer las disposiciones administrativas, técnicas y operativas para la gestión integral del Servicio de Vigilancia Electrónica y el uso de Dispositivos de Vigilancia Electrónica, en cumplimiento de las disposiciones emitidas por autoridad judicial competente, incluyendo los procedimientos de verificación, instalación, activación, monitoreo, atención de alertas y alarmas, soporte técnico, desinstalación, control de calidad, gestión de dispositivos dañados, así como los mecanismos de exoneración, reducción y diferimiento de pago, cuando corresponda.

Artículo 2.- Ámbito de aplicación. Las disposiciones contenidas en el presente Reglamento Técnico serán de cumplimiento obligatorio para las unidades administrativas, servidores públicos, personal técnico, operadores de monitoreo, supervisores, responsables territoriales y demás servidores del SNAI que intervengan en la gestión del Servicio de Vigilancia Electrónica y en la administración, control, seguimiento, instalación, monitoreo, soporte o desinstalación de Dispositivos de Vigilancia Electrónica.

Artículo 3.- Responsabilidad institucional. La Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, o quien haga sus veces, será responsable de coordinar, supervisar y ejecutar las acciones necesarias para la correcta gestión del Servicio de Vigilancia Electrónica, conforme las competencias institucionales, la normativa vigente y los lineamientos establecidos en el Reglamento Técnico que se expide mediante la presente Resolución.

Artículo 4.- Cumplimiento obligatorio. El Reglamento Técnico, sus anexos, formatos, instructivos y matrices serán de cumplimiento obligatorio para los servidores públicos y personal que intervenga directa o indirectamente en la gestión del Servicio de Vigilancia Electrónica, sin perjuicio de las responsabilidades administrativas, civiles o penales que pudieren derivarse por su inobservancia.

Artículo 5.- Componentes del Reglamento Técnico. El Reglamento Técnico estará conformado, al menos, por los siguientes componentes:

a. Gestión general del Servicio de Vigilancia Electrónica;
b. Verificación de disposiciones judiciales;
c. Instalación de Dispositivos de Vigilancia Electrónica bajo modalidad de libre circulación;
d. Instalación de Dispositivos de Vigilancia Electrónica bajo modalidad de arresto domiciliario;
e. Activación, vinculación y parametrización de dispositivos en la plataforma de monitoreo;
f. Monitoreo permanente de Dispositivos de Vigilancia Electrónica;
g. Atención, evaluación, clasificación, escalamiento, seguimiento y cierre de alertas y alarmas;
h. Control de calidad del monitoreo y atención de alarmas;
i. Soporte técnico, desinstalación y desvinculación de dispositivos;
j. Gestión de Dispositivos de Vigilancia Electrónica dañados;
k. Determinación, verificación y control del pago por concepto de uso y mantenimiento del Dispositivo de Vigilancia Electrónica, así como los procedimientos de exoneración, reducción o diferimiento del pago, conforme la normativa vigente;
l. Registro, archivo, trazabilidad documental y custodia de expedientes; y,
m. Los demás procedimientos, formatos, matrices o instructivos que sean necesarios para la correcta gestión del servicio.
n. Coordinación interinstitucional y comunicaciones con autoridad competente;
o. Supervisión, responsabilidades y mejora continua.

Artículo 6.- Principios aplicables. La gestión del Servicio de Vigilancia Electrónica se regirá por los principios de legalidad, eficacia, eficiencia, calidad, coordinación, responsabilidad, seguridad jurídica, trazabilidad, proporcionalidad, control, confidencialidad de la información, mejora continua y cumplimiento oportuno de las disposiciones judiciales.

Artículo 7.- Coordinación institucional. Las unidades administrativas del SNAI que intervengan en la gestión del Servicio de Vigilancia Electrónica deberán coordinar sus actuaciones de manera oportuna y articulada, a fin

de garantizar la instalación, activación, monitoreo, atención de eventos, soporte técnico, desinstalación, control de calidad y demás acciones necesarias para el cumplimiento de las disposiciones judiciales.

Cuando la naturaleza del evento lo requiera, la coordinación podrá realizarse con autoridad judicial competente, Fiscalía General del Estado, Policía Nacional, ECU 91, Consejo de la Judicatura u otras instituciones públicas competentes, de conformidad con la normativa vigente y los protocolos institucionales aplicables.

Artículo 8.- Segregación de funciones. La gestión del Servicio de Vigilancia Electrónica observará el principio de segregación de funciones, como regla general de control operativo, trazabilidad, seguridad de la información y prevención de concentración de actividades críticas. Para el efecto, deberán diferenciarse, conforme la naturaleza de cada procedimiento, las actividades de verificación documental, instalación física, activación lógica, parametrización, monitoreo, soporte técnico, control de calidad, supervisión, archivo y custodia documental.

La aplicación operativa de este principio deberá considerarse en los procedimientos de instalación, activación, parametrización, monitoreo, soporte, desinstalación y demás actuaciones vinculadas al servicio. En ningún caso una sola persona podrá concentrar todas las funciones críticas de un mismo procedimiento, salvo situaciones excepcionales debidamente justificadas, autorizadas y documentadas por la unidad responsable.

Artículo 9.- Uso obligatorio de formatos institucionales. Los informes, actas, matrices, bitácoras, registros, anexos fotográficos, documentos de soporte y demás instrumentos derivados de la gestión del Servicio de Vigilancia Electrónica deberán elaborarse utilizando los formatos institucionales aprobados o los que se emitan para el efecto.

La Dirección responsable podrá actualizar dichos formatos conforme las necesidades operativas, técnicas, normativas o de mejora continua del servicio.

CAPÍTULO II

DE LA VERIFICACIÓN DE DISPOSICIONES JUDICIALES

Artículo 10.- Recepción de disposiciones judiciales. La gestión del Servicio de Vigilancia Electrónica iniciará con la recepción de la disposición, resolución, providencia u orden judicial emitida por autoridad competente, mediante la cual se disponga el uso, instalación, activación, desinstalación, modificación, suspensión o cualquier otra actuación relacionada con el Dispositivo de Vigilancia Electrónica.

La recepción de la disposición judicial deberá efectuarse a través de los canales institucionales autorizados, debiendo registrarse la fecha y hora de ingreso, autoridad requirente, número de causa, datos de identificación de la persona, modalidad dispuesta y demás información necesaria para su trámite.

Artículo 11.- Verificación preliminar de la disposición judicial. Recibida la disposición judicial, la unidad responsable deberá verificar que el documento contenga la información mínima necesaria para su ejecución, entre la cual constará:

a. Identificación de la autoridad judicial competente;
b. Número de causa o proceso judicial;
c. Nombres, apellidos y número de identificación de la persona respecto de quien se dispone el uso del DVE;
d. Modalidad de vigilancia electrónica dispuesta, sea libre circulación, arresto domiciliario u otra determinada por autoridad competente;
e. Dirección exacta del domicilio, cuando se trate de arresto domiciliario;
f. Condiciones, restricciones, geocercas, horarios o reglas impuestas por la autoridad judicial;
g. Fecha de emisión de la disposición judicial;
h. Firma o validación correspondiente de la autoridad competente; y,

i. Demás información necesaria para la instalación, activación, monitoreo o desinstalación del dispositivo.

Artículo 12.- Validación de competencia y ejecutabilidad. La unidad responsable verificará que la disposición judicial provenga de autoridad competente y que sea clara, expresa y ejecutable. Para el efecto, se revisará que no existan errores sustanciales, inconsistencias, omisiones o contradicciones que impidan la instalación, activación, parametrización o monitoreo del Dispositivo de Vigilancia Electrónica.

Cuando la disposición judicial cumpla con los requisitos mínimos, se continuará con el procedimiento correspondiente, de acuerdo con la modalidad dispuesta.

Artículo 13.- Errores u omisiones en la disposición judicial. Cuando la disposición judicial contenga errores sustanciales, omisiones o información contradictoria respecto de los datos personales, número de causa, dirección de domicilio u otros elementos necesarios para su ejecución, la unidad responsable no procederá con la instalación, activación o modificación del DVE hasta que la autoridad judicial competente aclare, complete o rectifique la disposición.

En estos casos, se deberá comunicar la novedad a la autoridad judicial competente, dejando constancia documental de la imposibilidad de ejecución y de la información que requiere aclaración.

Artículo 14.- Registro de la disposición judicial. Toda disposición judicial recibida deberá ser registrada en la matriz, sistema, bitácora o expediente correspondiente, conforme los formatos institucionales establecidos para el efecto. El registro deberá permitir identificar, al menos, la fecha de ingreso, número de causa, autoridad judicial, datos del usuario, modalidad dispuesta, estado del trámite, responsable asignado y acciones ejecutadas.

Artículo 15.- Priorización de atención. La unidad responsable priorizará la atención de las disposiciones judiciales relacionadas con el uso de Dispositivos de Vigilancia Electrónica, considerando la fecha y hora de recepción, la modalidad dispuesta, la situación jurídica de la persona, la disponibilidad de dispositivos, la criticidad del caso y las instrucciones específicas emitidas por autoridad judicial competente.

En caso de existir imposibilidad material, técnica, logística u operativa para la atención inmediata de la disposición judicial, dicha novedad deberá ser registrada y comunicada a la autoridad competente, con la debida motivación.

Artículo 16.- Informe de factibilidad técnica. Se realizará en las modalidades de arresto domiciliario, libre circulación y en aquellos casos en que se requiera verificar condiciones técnicas, operativas o logísticas para la instalación del DVE, el personal técnico asignado elaborará el informe de factibilidad técnica correspondiente.

El informe deberá contener, al menos, los datos de la persona, número de causa, autoridad judicial, lugar de instalación, fecha de visita, condiciones técnicas verificadas, disponibilidad de señal, novedades identificadas, criterio técnico de viabilidad o no viabilidad y anexos de respaldo.

CAPÍTULO III

DE LA INSTALACIÓN DE DISPOSITIVOS DE VIGILANCIA ELECTRÓNICA

Artículo 17.- Procedencia de la instalación. La instalación del Dispositivo de Vigilancia Electrónica procederá únicamente cuando exista disposición judicial emitida por autoridad competente y cuando la misma sea clara, expresa y ejecutable.

Previo a la instalación, la unidad responsable deberá verificar la identidad de la persona, la modalidad dispuesta, la disponibilidad del dispositivo, las condiciones técnicas mínimas y la documentación necesaria para la ejecución del procedimiento. Asimismo, deberán observarse las reglas sobre pago, exoneración, reducción o

diferimiento previstas en el Capítulo correspondiente del presente Reglamento Técnico, sin reproducir en este Capítulo el procedimiento financiero aplicable.

Artículo 18.- Modalidades de instalación. La instalación de Dispositivos de Vigilancia Electrónica podrá ejecutarse bajo las siguientes modalidades:

a. Libre circulación: cuando la autoridad judicial disponga el uso del DVE permitiendo la movilidad de la persona dentro de las condiciones, horarios, restricciones o geocercas determinadas; y,
b. Arresto domiciliario: cuando la autoridad judicial disponga que la persona permanezca en el domicilio señalado, bajo control mediante Dispositivo de Vigilancia Electrónica.

Las modalidades deberán ser ejecutadas conforme lo ordenado por la autoridad judicial competente y de acuerdo con los procedimientos técnicos definidos por este Reglamento.

Artículo 19.- Plazo para la instalación. Notificada la disposición judicial que ordene el uso del Dispositivo de Vigilancia Electrónica, la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, a través de la gestión de Dispositivos de Vigilancia Electrónica, coordinará la entrega, instalación y activación del dispositivo en el término máximo de dos (2) días, conforme la normativa vigente.

La ejecución de la entrega, instalación y activación estará sujeta a la verificación previa de los requisitos administrativos, técnicos, operativos, financieros y documentales previstos en el presente Reglamento Técnico, según corresponda a la modalidad dispuesta por la autoridad judicial competente.

Cuando existan circunstancias que impidan cumplir dicho término, la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, a través de la gestión de Dispositivos de Vigilancia Electrónica, dejará constancia documentada de la novedad y comunicará el particular a la autoridad judicial competente, conforme las reglas de comunicación previstas en el Capítulo XI del presente Reglamento Técnico.

La imposibilidad de cumplir el término señalado deberá encontrarse debidamente respaldada en los registros, informes, actas, comunicaciones o documentos que correspondan, sin perjuicio de que se continúe con la gestión institucional necesaria para ejecutar la disposición judicial una vez superada la causa que impidió su cumplimiento oportuno.

Artículo 20.- Instalación bajo modalidad de libre circulación. En los casos de libre circulación, la persona deberá comparecer al punto autorizado por el SNAI para la instalación del Dispositivo de Vigilancia Electrónica, conforme la coordinación efectuada por la unidad responsable.

El personal técnico verificará la identidad de la persona, procederá con la colocación física del dispositivo, realizará las pruebas básicas de funcionamiento, suscribirá el acta correspondiente y coordinará la activación lógica y parametrización del dispositivo en la plataforma de monitoreo.

Artículo 21.- No comparecencia para instalación en libre circulación. Cuando la persona no comparezca al punto autorizado para la instalación del DVE dentro del plazo establecido o de la fecha coordinada, se dejará constancia de la novedad y se comunicará a la autoridad judicial competente, a fin de que adopte las decisiones que correspondan en el marco de sus atribuciones.

La no comparecencia deberá registrarse en la matriz, bitácora o sistema institucional correspondiente.

Artículo 22.- Instalación bajo modalidad de arresto domiciliario. En los casos de arresto domiciliario, el personal técnico asignado coordinará la logística necesaria para acudir al domicilio señalado en la disposición judicial, a fin de verificar las condiciones técnicas y ejecutar la instalación del Dispositivo de Vigilancia Electrónica.

El técnico responsable deberá verificar la identidad de la persona, la dirección dispuesta por autoridad judicial, las condiciones de conectividad, la viabilidad técnica de instalación, la colocación física del dispositivo, la elaboración del acta correspondiente y el levantamiento del informe de factibilidad técnica, cuando corresponda.

Artículo 23.- Imposibilidad de instalación en arresto domiciliario. Cuando no sea posible ejecutar la instalación del DVE en la modalidad de arresto domiciliario por ausencia de la persona, dirección incorrecta, imposibilidad de acceso al domicilio, falta de condiciones técnicas, negativa de colaboración, errores en la disposición judicial u otra causa debidamente justificada, el personal técnico deberá elaborar el informe correspondiente y remitirlo a la unidad responsable.

La unidad responsable comunicará la novedad a la autoridad judicial competente, adjuntando los respaldos necesarios.

Artículo 24.- Acta de entrega-recepción y acuerdo de uso del Dispositivo de Vigilancia Electrónica. Toda entrega del Dispositivo de Vigilancia Electrónica deberá respaldarse mediante el acta de entrega-recepción y acuerdo de uso correspondiente, documento que será suscrito por la persona portadora del dispositivo, el técnico responsable y demás intervinientes, cuando corresponda.

En dicho documento se dejará constancia, al menos, de la siguiente información:

a. Datos de identificación de la persona portadora del Dispositivo de Vigilancia Electrónica;
b. Número de causa o proceso judicial;
c. Autoridad judicial que dispuso el uso del dispositivo;
d. Modalidad de vigilancia electrónica dispuesta;
e. Número de serie, código o identificación del dispositivo entregado;
f. Fecha, hora y lugar de entrega y colocación del dispositivo;
g. Condiciones generales de uso, cuidado, conservación, carga y funcionamiento del dispositivo;
h. Obligaciones de la persona portadora del dispositivo;
i. Prohibiciones relacionadas con la manipulación, daño, pérdida, corte, retiro, desconexión, alteración o uso indebido del dispositivo;
j. Advertencia sobre las consecuencias administrativas o judiciales que podrían derivarse del incumplimiento de las condiciones de uso o de la disposición emitida por autoridad competente;
k. Constancia de la información brindada al usuario respecto del uso adecuado del dispositivo, conforme los artículos 25 y 32 del presente Reglamento Técnico;
l. Firma de la persona portadora del dispositivo, del técnico responsable y de los demás intervinientes, cuando corresponda; y,
m. Anexos fotográficos o documentales de respaldo, de ser aplicable.

La suscripción del acta de entrega-recepción y acuerdo de uso no sustituye la disposición judicial que ordena el uso del dispositivo, sino que constituye el respaldo administrativo, técnico y documental de la entrega, colocación, aceptación de condiciones de uso y obligaciones asumidas por la persona portadora del Dispositivo de Vigilancia Electrónica.

Artículo 25.- Capacitación al usuario. Al momento de la instalación, el personal técnico deberá informar a la persona portadora del DVE sobre el uso adecuado, carga, cuidado, conservación, restricciones, obligaciones, señales del dispositivo, alertas, alarmas y consecuencias derivadas de la manipulación, daño, pérdida, corte, desconexión o incumplimiento de las condiciones impuestas por la autoridad judicial.

La capacitación deberá quedar registrada en el acta correspondiente o en el formato institucional definido para el efecto.

Artículo 26.- Ejecución técnica de la instalación. El proceso de instalación del Dispositivo de Vigilancia Electrónica deberá ejecutarse de forma documentada, segura y trazable, tomando en cuenta la segregación de

funciones prevista en el artículo 8 del presente Reglamento Técnico, sin reproducir nuevamente la distribución general de actividades allí establecida.

Durante la colocación física del dispositivo, el técnico responsable deberá adoptar medidas de seguridad operativa orientadas a preservar la integridad del mecanismo de cierre, herramientas, accesorios, parámetros técnicos y demás elementos sensibles del procedimiento. Para este efecto, podrá solicitar al usuario que dirija su atención hacia un punto distinto al área específica de instalación mientras se ejecuta la colocación, ajuste o cierre del equipo, dejando constancia de cualquier novedad relevante en el acta o registro correspondiente.

Cuando la instalación requiera traslado de personal técnico, equipos o dispositivos hacia centros de privación de libertad, domicilios, unidades judiciales, puntos autorizados u otros lugares definidos para el cumplimiento de la disposición judicial, la unidad responsable coordinará, en los casos necesarios, la asignación del vehículo institucional correspondiente, conforme la disponibilidad logística, la planificación operativa y los procedimientos administrativos aplicables.

Artículo 27.- Verificación de identidad de la persona. Previo a la instalación del Dispositivo de Vigilancia Electrónica, el personal técnico asignado deberá verificar la identidad de la persona respecto de quien se dispuso la medida, beneficio, régimen o condición judicial, contrastando los datos constantes en la disposición judicial con el documento de identificación correspondiente.
Cuando exista inconsistencia entre la identidad de la persona y la información contenida en la disposición judicial, el procedimiento no podrá ejecutarse hasta que la autoridad competente aclare o rectifique la información respectiva.

Artículo 28.- Activación lógica del dispositivo. La activación lógica del Dispositivo de Vigilancia Electrónica en la plataforma institucional será ejecutada por el operador de plataforma o servidor autorizado, una vez colocada físicamente la unidad y verificada la información necesaria para su vinculación.

La activación deberá incluir, al menos, la asociación del dispositivo con la persona monitoreada, registro del número de serie, modalidad de vigilancia, autoridad judicial competente, número de causa, fecha de instalación y demás datos requeridos por el sistema institucional.

Artículo 29.- Parametrización de reglas de monitoreo. La parametrización del Dispositivo de Vigilancia Electrónica deberá realizarse conforme las condiciones expresamente dispuestas por la autoridad judicial competente, incluyendo zonas de inclusión, zonas de exclusión, horarios, restricciones de movilidad, perímetros, puntos autorizados y demás reglas aplicables.
Cuando la disposición judicial no contenga parámetros suficientes para configurar las reglas de monitoreo, la unidad responsable solicitará la aclaración correspondiente a la autoridad judicial competente, sin perjuicio de registrar la novedad en el expediente.

Artículo 30.- Validación inicial del funcionamiento. Una vez instalado y activado el Dispositivo de Vigilancia Electrónica, el personal técnico y el operador de plataforma deberán verificar que el equipo transmita señal correctamente, se encuentre vinculado a la persona monitoreada y refleje los parámetros configurados en la plataforma institucional.

La validación inicial deberá constar en el acta, informe, bitácora o registro correspondiente, dejando evidencia de la fecha, hora, responsable de verificación y resultado de las pruebas realizadas.

Artículo 31.- Respaldos probatorios de la actuación técnica. En toda instalación, desinstalación, soporte técnico, sustitución o reposición de Dispositivo de Vigilancia Electrónica deberá incorporarse un anexo fotográfico que respalde la actuación realizada.

En toda instalación, desinstalación, soporte técnico, sustitución o reposición de Dispositivo de Vigilancia Electrónica deberán incorporarse respaldos probatorios suficientes que permitan verificar la actuación técnica ejecutada, observando criterios de necesidad, proporcionalidad, seguridad y reserva de la información.

Los respaldos probatorios comprenderán, cuando corresponda, el anexo fotográfico de la actuación realizada y el registro de ubicación o georreferenciación de la visita técnica, siempre que sea técnicamente posible.

Dichos respaldos deberán integrarse al expediente correspondiente y permitir verificar el lugar, fecha, hora, técnico asignado, actuación realizada y demás elementos necesarios, evitando la difusión o uso no autorizado de imágenes, datos personales o información sensible.

Artículo 32.- Información al usuario sobre uso del dispositivo. La persona portadora del Dispositivo de Vigilancia Electrónica deberá recibir información clara sobre el uso adecuado del equipo, obligaciones de carga, cuidado, conservación, prohibición de manipulación, consecuencias por daño, pérdida, corte, desconexión, incumplimiento de geocercas, pérdida de señal injustificada y demás condiciones aplicables.

La unidad responsable podrá entregar material informativo físico o digital, como trípticos, guías o instructivos, que contengan recomendaciones para el uso, cuidado y conservación del dispositivo.

Artículo 33.- Obligaciones de la persona portadora del DVE. La persona portadora del Dispositivo de Vigilancia Electrónica tendrá, al menos, las siguientes obligaciones:

a. Usar el dispositivo conforme las instrucciones impartidas por el personal técnico y las condiciones dispuestas por autoridad judicial competente;
b. Mantener el dispositivo encendido, cargado y en condiciones adecuadas de funcionamiento;
c. No manipular, cortar, abrir, retirar, golpear, alterar, mojar, cubrir, bloquear o desconectar el dispositivo;
d. No impedir la transmisión de señal GPS, GSM o cualquier otro mecanismo de localización o comunicación del equipo;
e. Cumplir las zonas, horarios, perímetros, restricciones y condiciones impuestas por la autoridad judicial competente;
f. Atender las llamadas, comunicaciones o requerimientos efectuados por el personal de monitoreo, soporte técnico o autoridad competente;
g. Reportar oportunamente cualquier daño, falla, pérdida, robo, deterioro o novedad relacionada con el dispositivo;
h. Comparecer a los puntos autorizados cuando sea requerido para revisión, soporte, sustitución, reposición o desinstalación;
i. Permitir la ejecución de visitas técnicas o verificaciones necesarias, cuando corresponda; y,
j. Las demás obligaciones establecidas en la disposición judicial, normativa vigente, actas, instructivos o documentos institucionales aplicables.

Artículo 34.- Prohibiciones de la persona portadora del DVE. La persona portadora del Dispositivo de Vigilancia Electrónica tendrá prohibido:

a. Retirar, cortar, manipular, alterar o inutilizar el dispositivo;
b. Permitir que terceras personas manipulen el equipo;
c. Ocultar, bloquear o impedir la transmisión de señal del dispositivo;
d. Trasladarse fuera de las zonas autorizadas o ingresar a zonas restringidas, salvo autorización judicial competente;
e. Incumplir los horarios, restricciones o condiciones impuestas por autoridad judicial;
f. Negarse injustificadamente a recibir soporte técnico, revisión, sustitución o desinstalación del dispositivo;
g. Proporcionar información falsa, incompleta o inexacta al personal responsable; y,
h. Cualquier otra acción u omisión que afecte la finalidad del Sistema de Vigilancia Electrónica o el cumplimiento de la disposición judicial.

Artículo 35.- Comunicación de instalación a la autoridad judicial. Ejecutada la instalación, activación y validación inicial del Dispositivo de Vigilancia Electrónica, la unidad responsable comunicará a la autoridad judicial competente el cumplimiento de la disposición, conforme las reglas de comunicación previstas en el

Capítulo XI del presente Reglamento Técnico.

La comunicación deberá adjuntar el acta de entrega-recepción y acuerdo de uso, el respaldo de activación y validación inicial, y los demás documentos o novedades relevantes del procedimiento, según corresponda.

CAPÍTULO IV

DEL MONITOREO DE LOS DISPOSITIVOS DE VIGILANCIA ELECTRÓNICA

Artículo 36.- Monitoreo permanente. El monitoreo de los Dispositivos de Vigilancia Electrónica se realizará de manera permanente, las veinticuatro horas del día, los trescientos sesenta y cinco días del año, a través del Centro de Monitoreo o la unidad operativa que corresponda, conforme las competencias institucionales y los procedimientos establecidos para el efecto.

El monitoreo tendrá por finalidad verificar el cumplimiento de las condiciones impuestas por autoridad judicial competente, identificar eventos, alertas, alarmas o novedades, y activar las acciones operativas que correspondan según el nivel de criticidad del evento.

Artículo 37.- Responsabilidad del personal de monitoreo. El personal de monitoreo será responsable de observar, registrar, validar, gestionar y dar seguimiento a los eventos generados por los Dispositivos de Vigilancia Electrónica en la plataforma institucional.

Para el cumplimiento de sus funciones, deberá actuar con oportunidad, diligencia, reserva, objetividad, trazabilidad y apego a los procedimientos internos, dejando constancia documental de las acciones ejecutadas durante su turno.

Artículo 38.- Supervisión del monitoreo. El supervisor de monitoreo será responsable de controlar la correcta gestión de los eventos generados en la plataforma, verificar la atención oportuna de alertas y alarmas, validar los reportes de novedades, disponer el escalamiento de eventos críticos y coordinar las acciones necesarias con las unidades internas o instituciones externas competentes.

El supervisor deberá asegurar que los operadores de monitoreo cumplan los tiempos de atención, registros, protocolos de comunicación, criterios de clasificación y demás lineamientos establecidos en el Reglamento Técnico y en los instructivos específicos.

Artículo 39.- Plataforma del Sistema de Vigilancia Electrónica. La Plataforma del Sistema de Vigilancia Electrónica será el medio tecnológico principal para el seguimiento, control, registro y gestión de los Dispositivos de Vigilancia Electrónica.

En dicha plataforma se deberá registrar la información relacionada con usuarios monitoreados, dispositivos asignados, modalidad de vigilancia, reglas de monitoreo, geocercas, alertas, alarmas, eventos, novedades, comunicaciones, acciones ejecutadas y cierre de eventos, según corresponda.

Artículo 40.- Bitácora y registro de novedades. La bitácora de monitoreo constituirá un instrumento obligatorio de registro, control y trazabilidad de las actuaciones ejecutadas por el personal de monitoreo.

El personal de monitoreo deberá registrar de manera clara, completa y oportuna las novedades identificadas durante su turno, incluyendo eventos técnicos, alertas, alarmas, pérdida de señal, batería baja, manipulación, salida o ingreso a geocercas, incumplimientos, comunicaciones con usuarios, coordinaciones institucionales y cualquier otra situación relevante.
La bitácora deberá contener, al menos:

a. Fecha y turno de monitoreo;
b. Identificación del operador responsable;
c. Número de dispositivo o identificación del usuario monitoreado;
d. Tipo de evento, alerta o alarma;
e. Hora de generación del evento;
f. Hora de atención;
g. Acciones ejecutadas;
h. Resultado de la gestión;
i. Comunicaciones realizadas;
j. Escalamiento efectuado, cuando corresponda; y,
k. Observaciones relevantes.

Artículo 41.- Atención de eventos generados por el sistema. Todo evento generado por la Plataforma del Sistema de Vigilancia Electrónica deberá ser revisado por el operador de monitoreo, a fin de determinar si corresponde a una alerta, alarma, evento informativo, novedad técnica, posible incumplimiento o situación que requiera gestión institucional.

La atención del evento deberá realizarse conforme el nivel de criticidad, tiempos máximos de respuesta, protocolos de comunicación y procedimientos definidos en el Reglamento Técnico y en el instructivo específico de monitoreo, evaluación y gestión de alertas.

Artículo 42.- Gestión de pérdida de señal. Cuando se genere un evento de pérdida de señal del Dispositivo de Vigilancia Electrónica, el operador de monitoreo deberá verificar la naturaleza del evento, revisar antecedentes inmediatos, intentar contacto con la persona monitoreada y ejecutar las acciones que correspondan conforme el nivel de criticidad asignado.

Si la pérdida de señal se prolonga o no existe respuesta del usuario dentro del tiempo establecido, el operador deberá informar al supervisor de monitoreo para que se disponga el escalamiento correspondiente y, de ser procedente, la elaboración del informe de novedades y comunicación a la autoridad competente.

Artículo 43.- Gestión de batería baja. Cuando se genere una alerta por batería baja, el operador de monitoreo deberá comunicarse con la persona portadora del DVE, recordarle la obligación de mantener el dispositivo cargado y registrar la acción ejecutada.

Si la alerta persiste, se vuelve recurrente o genera riesgo de desconexión del dispositivo, el evento podrá ser escalado al supervisor de monitoreo para su seguimiento y eventual comunicación a la autoridad competente, según corresponda.

Artículo 44.- Gestión de manipulación, corte o daño del dispositivo. Cuando el sistema genere alertas o alarmas relacionadas con manipulación, corte, apertura, alteración, daño, impacto o posible inutilización del Dispositivo de Vigilancia Electrónica, el operador deberá tratar el evento como prioritario y ejecutar de manera inmediata las acciones de verificación, contacto, seguimiento y escalamiento.

En caso de confirmarse la manipulación, corte, daño o pérdida de control del dispositivo, la unidad responsable deberá elaborar el informe correspondiente y comunicar la novedad a la autoridad judicial competente, sin perjuicio de las acciones administrativas, técnicas o legales que correspondan.

Artículo 45.- Gestión de geocercas. El operador de monitoreo deberá verificar los eventos relacionados con salida de zona permitida, ingreso a zona restringida, incumplimiento de perímetros, permanencia fuera del área autorizada o cualquier otra novedad vinculada con geocercas configuradas por disposición judicial.

Cuando el evento pueda constituir incumplimiento de las condiciones impuestas por autoridad competente, deberá gestionarse conforme el nivel de criticidad, registrarse en el sistema y escalarse al supervisor de monitoreo, para la elaboración del informe y comunicación respectiva.

Artículo 46.- Contacto con la persona monitoreada. El contacto con la persona monitoreada deberá realizarse únicamente para fines institucionales vinculados con el seguimiento del DVE, verificación de eventos, gestión de alertas o alarmas, soporte técnico, cumplimiento de obligaciones o atención de novedades operativas.

Toda comunicación deberá registrarse en la plataforma, bitácora o formato correspondiente, indicando fecha, hora, número utilizado, responsable de la llamada, resultado del contacto y observaciones relevantes.

Artículo 47.- Falta de respuesta de la persona monitoreada. Cuando la persona monitoreada no responda a las llamadas, mensajes, comunicaciones o requerimientos realizados por el personal de monitoreo, dicha novedad deberá ser registrada y valorada conforme la naturaleza del evento.

Si la falta de respuesta se relaciona con una alerta o alarma de criticidad media, alta o crítica, el operador deberá informar al supervisor de monitoreo para que se disponga el escalamiento correspondiente y, de ser necesario, se comunique la novedad a la autoridad competente.

Artículo 48.- Informes de novedades de monitoreo. Los informes de novedades de monitoreo deberán elaborarse cuando se identifiquen eventos relevantes, incumplimientos, alertas críticas, alarmas, manipulación, corte, pérdida prolongada de señal, salida de geocerca, ingreso a zona restringida, falta de respuesta del usuario o cualquier otra circunstancia que pueda afectar el cumplimiento de la disposición judicial.

El informe deberá contener, al menos:

a. Datos de identificación de la persona monitoreada;
b. Número de causa o proceso judicial;
c. Autoridad judicial competente;
d. Número de serie del dispositivo;
e. Modalidad de vigilancia electrónica;
f. Descripción clara del evento;
g. Fecha y hora de generación;
h. Fecha y hora de atención;
i. Acciones ejecutadas por el operador;
j. Comunicaciones realizadas;
k. Resultado de la gestión;
l. Anexos o respaldos del sistema; y,
m. Conclusión o recomendación operativa, cuando corresponda.

Artículo 49.- Continuidad del monitoreo. La unidad responsable deberá adoptar las medidas necesarias para garantizar la continuidad del monitoreo de los Dispositivos de Vigilancia Electrónica, incluyendo la organización de turnos, supervisión operativa, disponibilidad de personal, acceso a la plataforma, registro de novedades y mecanismos de contingencia frente a fallas técnicas, interrupciones del sistema o eventos críticos.

Artículo 50.- Relevo de turno. El relevo de turno del personal de monitoreo deberá realizarse de manera ordenada, documentada y verificable, dejando constancia de las novedades pendientes, eventos en seguimiento, alertas activas, comunicaciones realizadas, casos críticos, dispositivos sin señal, usuarios sin contacto y demás asuntos que requieran continuidad operativa.

El operador entrante deberá revisar la información recibida y asumir la gestión de los eventos pendientes, sin afectar la continuidad del monitoreo.

Artículo 51.- Responsabilidad por omisión de gestión. La falta de atención, registro, seguimiento, escalamiento o comunicación oportuna de eventos, alertas, alarmas o novedades generadas por el Sistema de Vigilancia Electrónica podrá generar responsabilidades administrativas, civiles o penales, conforme la normativa vigente.

Resolución Nro. SNAI-SNAI-2026-0052-R

Quito, D.M., 15 de mayo de 2026

CAPÍTULO V

DE LA ATENCIÓN, CLASIFICACIÓN Y GESTIÓN DE ALERTAS Y ALARMAS

Artículo 52.- Atención de alertas y alarmas. La atención de alertas y alarmas comprende el conjunto de acciones técnicas, operativas y administrativas ejecutadas por el personal de monitoreo frente a eventos generados por los Dispositivos de Vigilancia Electrónica, que puedan representar riesgo de incumplimiento de la disposición judicial, pérdida de control del usuario monitoreado, manipulación del dispositivo, afectación a la seguridad del sistema o novedades técnicas que requieran gestión institucional.

La atención de alertas y alarmas deberá realizarse conforme los niveles de criticidad, tiempos de respuesta, procedimientos de verificación, escalamiento, seguimiento y cierre establecidos en el Reglamento Técnico y en el instructivo específico de monitoreo, evaluación y gestión de alertas.

Artículo 53.- Validación inicial de la alerta o alarma. Una vez generada una alerta o alarma en la Plataforma del Sistema de Vigilancia Electrónica, el operador de monitoreo deberá validar el evento, verificando su naturaleza, hora de generación, dispositivo involucrado, usuario monitoreado, modalidad de vigilancia, condiciones judiciales aplicables, ubicación reportada, historial inmediato de eventos y demás información disponible en el sistema.

La validación inicial permitirá determinar si el evento es procedente, no procedente, informativo, técnico, recurrente, crítico o si requiere escalamiento inmediato.

Artículo 54.- Criterios para la clasificación de alertas y alarmas. La clasificación de alertas y alarmas deberá fundamentarse, al menos, en los siguientes criterios:

a. Nivel de riesgo asociado al evento;
b. Impacto en la seguridad o control del usuario monitoreado;
c. Probabilidad de incumplimiento de las medidas dispuestas por autoridad judicial;
d. Condiciones operativas del dispositivo;
e. Historial de eventos del usuario monitoreado;
f. Posibilidad de contacto y verificación con la persona monitoreada;
g. Persistencia o recurrencia del evento;
h. Ubicación geográfica reportada por el sistema;
i. Modalidad de vigilancia electrónica aplicable; y,
j. Cualquier otro elemento técnico u operativo que permita valorar la criticidad del evento.

Artículo 55.- Niveles de criticidad. Las alertas y alarmas generadas por los Dispositivos de Vigilancia Electrónica se clasificarán, de manera general, en los siguientes niveles:

a. Nivel 1 - Crítico: eventos que representan riesgo alto o inminente para el cumplimiento de la disposición judicial, la continuidad del monitoreo o el control del usuario monitoreado;

b. Nivel 2 - Alto: eventos que pueden comprometer el cumplimiento de las condiciones judiciales o la operatividad del dispositivo, y que requieren atención prioritaria y posible escalamiento;

c. Nivel 3 - Medio: eventos que requieren verificación, contacto con el usuario o seguimiento operativo, sin que inicialmente representen una situación crítica; y,

d. Nivel 4 - Bajo: eventos informativos, técnicos o de bajo impacto operativo, que deben registrarse y gestionarse conforme corresponda.

Resolución Nro. SNAI-SNAI-2026-0052-R

Quito, D.M., 15 de mayo de 2026

Artículo 56.- Matriz de clasificación de alertas y alarmas. Para la atención de alertas y alarmas, el personal de monitoreo aplicará la siguiente matriz referencial de clasificación, sin perjuicio de los ajustes técnicos que puedan realizarse conforme la plataforma, tecnología utilizada o instructivos específicos:

Artículo 57.- Alarmas críticas. Serán consideradas alarmas críticas aquellas que representen riesgo alto o inminente para el cumplimiento de la disposición judicial, la continuidad del monitoreo, la integridad del dispositivo o el control del usuario monitoreado.

Se considerarán, entre otras, alarmas críticas:

a. Corte confirmado del dispositivo;
b. Manipulación confirmada del equipo;
c. Salida de geocerca crítica;
d. Ingreso a zona de exclusión de alta relevancia;
e. Pérdida prolongada de señal sin respuesta del usuario, cuando el contexto lo amerite;
f. Daño intencional o inutilización del dispositivo; y,
g. Cualquier evento que comprometa gravemente la finalidad del Sistema de Vigilancia Electrónica.

Las alarmas críticas deberán ser atendidas de forma inmediata, registradas en el sistema y escaladas al supervisor de monitoreo o autoridad institucional competente.

Artículo 58.- Alertas de nivel alto. Serán consideradas alertas de nivel alto aquellas que, sin constituir inicialmente una alarma crítica, puedan comprometer el cumplimiento de la disposición judicial, la continuidad del monitoreo o la operatividad del dispositivo.

Estas alertas deberán gestionarse de manera prioritaria mediante contacto con el usuario, verificación de ubicación, revisión del historial de eventos, seguimiento operativo y escalamiento cuando el evento persista, se agrave o no pueda ser justificado técnicamente.

Artículo 59.- Alertas de nivel medio. Serán consideradas alertas de nivel medio aquellas que requieran gestión operativa, contacto con el usuario o seguimiento del dispositivo, pero que no generen inicialmente un riesgo alto o inminente.

Entre estas podrán encontrarse eventos de batería baja, intermitencia de señal, golpes o impactos no confirmados, novedades técnicas menores o eventos que requieran validación adicional.

Artículo 60.- Alertas de nivel bajo o eventos informativos. Serán considerados eventos de nivel bajo aquellos que no impliquen afectación inmediata al cumplimiento de la disposición judicial ni a la continuidad del monitoreo, pero que deban ser registrados para fines de trazabilidad, control, análisis estadístico o seguimiento institucional.

Estos eventos deberán ser registrados en la plataforma, bitácora o matriz correspondiente.

Artículo 61.- Gestión de alertas procedentes. Una alerta o alarma será considerada procedente cuando, luego de la validación correspondiente, se determine que el evento generado tiene relación efectiva con una novedad real, incumplimiento, riesgo, manipulación, daño, pérdida de señal, salida o ingreso a geocerca, falta de respuesta del usuario o afectación operativa del dispositivo.

Las alertas o alarmas procedentes deberán ser gestionadas conforme su nivel de criticidad, aplicando las acciones de contacto, verificación, seguimiento, escalamiento, coordinación institucional, elaboración de informe y comunicación a la autoridad competente, cuando corresponda.

Artículo 62.- Gestión de alertas no procedentes. Una alerta o alarma será considerada no procedente cuando, luego de la validación correspondiente, se determine que el evento obedece a una falla técnica, error del sistema,

intermitencia momentánea, condición normal de operación, duplicidad de registro, evento automático sin impacto operativo u otra circunstancia verificable que descarte incumplimiento o riesgo.

La calificación de una alerta como no procedente deberá ser debidamente justificada y registrada en la plataforma institucional, bitácora o matriz correspondiente.

Artículo 63.- Escalamiento de alertas y alarmas. El escalamiento procederá cuando la alerta o alarma, por su nivel de criticidad, persistencia, recurrencia, imposibilidad de contacto con el usuario, afectación al dispositivo o presunto incumplimiento de la disposición judicial, requiera conocimiento o intervención del supervisor de monitoreo, autoridad institucional, área técnica, Policía Nacional, ECU 911, autoridad judicial competente u otra institución pública.

El escalamiento deberá realizarse de manera oportuna y documentada, dejando constancia de la fecha, hora, responsable, institución o servidor contactado, medio utilizado, acciones coordinadas y resultado obtenido.

Artículo 64.- Escalamiento interno. El escalamiento interno se realizará dentro del SNAI cuando el evento requiera intervención del supervisor de monitoreo, responsable del Centro de Monitoreo, soporte técnico, Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, o cualquier otra unidad administrativa competente.

Procederá especialmente en casos de eventos críticos, fallas técnicas recurrentes, pérdida prolongada de señal, manipulación, daño del dispositivo, falta de respuesta del usuario o eventos que requieran validación superior.

Artículo 65.- Seguimiento de alertas y alarmas. El operador de monitoreo deberá realizar seguimiento a las alertas y alarmas hasta que el evento sea atendido, controlado, justificado, escalado o cerrado conforme el procedimiento correspondiente.

En eventos críticos o de nivel alto, el seguimiento deberá mantenerse hasta contar con una respuesta operativa, comunicación efectiva, intervención institucional, recuperación de señal, regularización del evento o disposición superior.

Artículo 66.- Cierre de alertas y alarmas. El cierre de una alerta o alarma procederá únicamente cuando el evento haya sido atendido, verificado, controlado, justificado o escalado conforme corresponda.

El cierre deberá registrarse en el sistema, indicando:

a. Fecha y hora de cierre;
b. Responsable del cierre;
c. Tipo de evento;
d. Nivel de criticidad asignado;
e. Acciones ejecutadas;
f. Resultado de la gestión;
g. Justificación del cierre;
h. Comunicaciones realizadas; y,
i. Observaciones relevantes.

En eventos críticos, el cierre podrá requerir validación del supervisor de monitoreo.

Artículo 67.- Registro obligatorio de la gestión. Toda alerta, alarma o evento generado por el Sistema de Vigilancia Electrónica deberá contar con registro de gestión, independientemente de que sea procedente, no procedente, técnico, informativo, crítico o de bajo impacto.

El registro deberá garantizar la trazabilidad del evento desde su generación hasta su cierre, incluyendo hora de generación, hora de atención, responsable, acciones ejecutadas, resultado, escalamiento y respaldo documental.

Artículo 68.- Prohibición de cierre injustificado. Queda prohibido cerrar, eliminar, modificar o justificar alertas, alarmas o eventos sin haber realizado la validación, gestión y registro correspondiente.

CAPÍTULO VI

DEL CONTROL DE CALIDAD DEL MONITOREO Y ATENCIÓN DE ALARMAS

Artículo 69.- Control de calidad del monitoreo. El control de calidad del monitoreo comprende las acciones de revisión, verificación, evaluación y seguimiento destinadas a comprobar que la atención de eventos, alertas, alarmas y novedades generadas por los Dispositivos de Vigilancia Electrónica se realice conforme los procedimientos institucionales, tiempos de respuesta, criterios de clasificación, registros obligatorios y protocolos de escalamiento establecidos.

La unidad responsable deberá implementar mecanismos de control que permitan evaluar la oportunidad, eficiencia, trazabilidad y calidad de la gestión ejecutada por el personal de monitoreo.

Artículo 70.- Finalidad del control de calidad. El control de calidad tendrá como finalidad fortalecer la gestión del Servicio de Vigilancia Electrónica, identificar oportunidades de mejora, prevenir omisiones operativas, verificar el cumplimiento de estándares institucionales y garantizar que los eventos generados por el sistema sean atendidos de manera adecuada, oportuna y documentada.

Artículo 71.- Responsables del control de calidad. El control de calidad estará a cargo del servidor, equipo o unidad designada por la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, o quien haga sus veces, sin perjuicio de la supervisión que corresponda a los responsables del Centro de Monitoreo y demás autoridades institucionales competentes.

El personal encargado del control de calidad deberá actuar con objetividad, reserva, independencia técnica y apego a los procedimientos institucionales.

Artículo 72.- Alcance de la revisión de calidad. La revisión de calidad podrá comprender, entre otros aspectos:

a. Atención oportuna de alertas y alarmas;
b. Correcta clasificación del nivel de criticidad;
c. Cumplimiento de tiempos máximos de respuesta;
d. Registro completo de acciones ejecutadas;
e. Escalamiento interno o externo cuando corresponda;
f. Elaboración y remisión de informes de novedades;
g. Cierre adecuado y justificado de eventos;
h. Seguimiento de eventos críticos o recurrentes;
i. Coordinación con instituciones externas;
j. Uso correcto de bitácoras, matrices y plataforma institucional; y,
k. Cumplimiento de protocolos de reserva y seguridad de la información.

Artículo 73.- Revisión de eventos críticos. Los eventos críticos deberán ser objeto de revisión prioritaria dentro del proceso de control de calidad, especialmente aquellos relacionados con corte del dispositivo, manipulación confirmada, salida de geocerca crítica, ingreso a zona restringida, pérdida prolongada de señal sin respuesta del usuario, evasión o posible incumplimiento de la disposición judicial.

La revisión deberá verificar si el evento fue atendido oportunamente, si se realizó el escalamiento correspondiente, si se dejó constancia documental suficiente y si se comunicó a la autoridad competente, cuando

correspondía.

Artículo 74.- Revisión de eventos cerrados. Los eventos cerrados en la plataforma institucional podrán ser revisados para verificar que el cierre haya sido debidamente justificado y respaldado.
No se considerará válido el cierre de alertas, alarmas o eventos cuando no exista registro de validación, acción ejecutada, resultado de la gestión, justificación técnica u operativa, o identificación del responsable del cierre.

Artículo 75.- Evaluación del cumplimiento de estándares. El control de calidad deberá evaluar el cumplimiento de los estándares mínimos establecidos para la gestión de monitoreo, incluyendo tiempos de respuesta, trazabilidad, registro documental, clasificación de eventos, escalamiento, elaboración de informes y comunicación institucional.

Los resultados de la evaluación deberán servir como insumo para la mejora continua del Servicio de Vigilancia Electrónica.

Artículo 76.- Identificación de hallazgos. Cuando en el proceso de control de calidad se identifiquen omisiones, inconsistencias, retrasos, errores de clasificación, registros incompletos, cierres injustificados, falta de escalamiento, ausencia de informes o incumplimiento de procedimientos, se generará el hallazgo correspondiente.

Los hallazgos deberán clasificarse según su naturaleza, impacto y nivel de riesgo operativo, sin perjuicio de las responsabilidades administrativas que pudieren derivarse.

Artículo 77.- Clasificación de hallazgos. Los hallazgos derivados del control de calidad podrán clasificarse, de manera general, en:

a. Hallazgos leves: inconsistencias formales, errores de registro o incumplimientos menores que no comprometan la atención del evento ni la finalidad del monitoreo;
b. Hallazgos moderados: omisiones o errores que afecten la trazabilidad, oportunidad o calidad de la gestión, sin generar un riesgo crítico inmediato; y,
c. Hallazgos graves: omisiones, retrasos, cierres injustificados, falta de escalamiento o ausencia de comunicación que puedan comprometer el cumplimiento de una disposición judicial, la seguridad del sistema o la continuidad del monitoreo.

Artículo 78.- Informe de control de calidad. Los resultados del control de calidad deberán constar en un informe técnico o matriz institucional, en el que se detalle, al menos:

a. Período evaluado;
b. Responsable de la revisión;
c. Número de eventos revisados;
d. Tipo de alertas o alarmas evaluadas;
e. Cumplimiento de tiempos de respuesta;
f. Hallazgos identificados;
g. Acciones correctivas recomendadas;
h. Responsables de implementación;
i. Plazos sugeridos de cumplimiento; y,
j. Conclusiones y recomendaciones.

Artículo 79.- Acciones correctivas. Cuando se identifiquen hallazgos o incumplimientos en la gestión de monitoreo, la unidad responsable deberá disponer o recomendar las acciones correctivas necesarias, orientadas a subsanar las deficiencias detectadas, prevenir su recurrencia y fortalecer la calidad del servicio.

La definición, implementación y seguimiento de las acciones correctivas se sujetará a la regulación general prevista en el artículo 181 del presente Reglamento Técnico.

Artículo 80.- Seguimiento de acciones correctivas. Las acciones correctivas derivadas del control de calidad deberán ser objeto de seguimiento hasta verificar su cumplimiento.

El seguimiento deberá registrarse en la matriz, informe o sistema correspondiente, dejando constancia del responsable asignado, plazo de cumplimiento, estado de avance, evidencia presentada y resultado final.

Artículo 81.- Retroalimentación al personal de monitoreo. Los resultados del control de calidad podrán ser socializados con el personal de monitoreo, supervisores y responsables operativos, con la finalidad de fortalecer criterios de atención, mejorar la clasificación de eventos, corregir errores recurrentes y promover la aplicación uniforme de los procedimientos institucionales.

La retroalimentación deberá realizarse bajo un enfoque técnico, preventivo y de mejora continua, sin perjuicio de las acciones administrativas que correspondan en caso de incumplimientos graves.

Artículo 82.- Indicadores de calidad. La unidad responsable podrá establecer indicadores de calidad para evaluar el desempeño del monitoreo y atención de alarmas, tales como:

a. Porcentaje de alertas atendidas dentro del tiempo establecido;
b. Número de eventos críticos escalados oportunamente;
c. Porcentaje de eventos con registro completo;
d. Número de cierres observados o injustificados;
e. Número de informes emitidos por eventos relevantes;
f. Frecuencia de eventos recurrentes por usuario o dispositivo;
g. Cumplimiento de acciones correctivas; y,
h. Otros indicadores que permitan medir la calidad del servicio.

Artículo 83.- Registro y archivo del control de calidad. Los informes, matrices, respaldos, evidencias, hallazgos y acciones correctivas generadas dentro del proceso de control de calidad deberán ser registrados y archivados por la unidad responsable, conforme las reglas generales de registro, archivo, custodia y trazabilidad documental previstas en el Capítulo correspondiente del presente Reglamento Técnico.

CAPÍTULO VII

DEL SOPORTE TÉCNICO, DIAGNÓSTICO, SUSTITUCIÓN, REPOSICIÓN Y DESINSTALACIÓN DE DISPOSITIVOS DE VIGILANCIA ELECTRÓNICA

Artículo 84.- Soporte técnico de Dispositivos de Vigilancia Electrónica. El soporte técnico comprende las acciones de revisión, diagnóstico, mantenimiento, configuración, sustitución, reposición o atención de novedades técnicas relacionadas con los Dispositivos de Vigilancia Electrónica, sus accesorios, componentes, funcionamiento, conectividad, señal, batería, transmisión de datos o vinculación con la plataforma institucional.

El soporte técnico deberá ejecutarse de manera oportuna, documentada y conforme los procedimientos institucionales, garantizando la continuidad del monitoreo y la trazabilidad de la actuación realizada.

Artículo 85.- Procedencia del soporte técnico. El soporte técnico procederá cuando se identifiquen fallas, alertas técnicas, pérdida recurrente de señal, deterioro, daño, mal funcionamiento, batería defectuosa, errores de configuración, imposibilidad de transmisión, novedades reportadas por el usuario, alertas generadas por la plataforma o requerimientos efectuados por el personal de monitoreo, supervisor o autoridad competente.

Toda atención de soporte técnico deberá ser registrada en la plataforma, bitácora, matriz, informe o acta correspondiente.

Artículo 86.- Coordinación del soporte técnico. Cuando se requiera soporte técnico, la unidad responsable coordinará con el usuario monitoreado, personal técnico, operador de monitoreo, supervisor y demás intervinientes necesarios, a fin de ejecutar la revisión o atención correspondiente.

La coordinación deberá considerar la modalidad de vigilancia electrónica, ubicación del usuario, nivel de criticidad de la novedad, disponibilidad de personal técnico, disponibilidad de dispositivos y condiciones logísticas necesarias.

Artículo 87.- Soporte técnico en modalidad de libre circulación. En los casos de libre circulación, el soporte técnico podrá ejecutarse en los puntos autorizados por el SNAI a nivel nacional o en el lugar que determine la unidad responsable, conforme la naturaleza de la novedad y las condiciones operativas del caso.

El usuario deberá comparecer al punto autorizado cuando sea convocado para revisión, mantenimiento, sustitución, reposición, verificación o desinstalación del Dispositivo de Vigilancia Electrónica.

Artículo 88.- Soporte técnico en modalidad de arresto domiciliario. En los casos de arresto domiciliario, el soporte técnico podrá ejecutarse en el domicilio señalado en la disposición judicial o en el lugar autorizado por la autoridad competente, conforme las condiciones del caso y la modalidad impuesta.

Cuando se requiera visita técnica domiciliaria, el técnico asignado deberá documentar la actuación, registrar la georreferenciación cuando sea posible, levantar el acta o informe correspondiente e incorporar los anexos de respaldo al expediente.

Artículo 89.- Diagnóstico técnico y clasificación del estado del dispositivo. El personal técnico responsable deberá realizar el diagnóstico del Dispositivo de Vigilancia Electrónica, verificando su estado físico, funcionamiento, batería, conectividad, transmisión de señal, integridad del equipo, accesorios, correas, cierres, sensores, componentes y demás aspectos necesarios para determinar la novedad presentada.

El diagnóstico deberá concluir, de manera expresa, si el dispositivo se encuentra en estado bueno, regular o malo, conforme criterios técnicos verificables, sin perjuicio de que el equipo pueda requerir mantenimiento, sustitución, reposición, custodia o la activación de los procedimientos patrimoniales o administrativos que correspondan.

Para efectos del presente Reglamento Técnico, se considerará dispositivo en estado bueno aquel que se encuentre operativo, transmita señal, mantenga conectividad, conserve batería funcional, no presente daño físico relevante y permita su uso normal en el servicio. Se considerará dispositivo en estado regular aquel que funcione, pero evidencie desgaste material, deterioro superficial, fallas no críticas, disminución de rendimiento, requerimiento de mantenimiento preventivo o correctivo, o condiciones que no impidan inmediatamente el monitoreo, pero deban ser registradas y atendidas. Se considerará dispositivo en estado malo aquel que no funcione adecuadamente, no transmita señal, presente daño estructural, corte, manipulación, alteración, pérdida de componentes, batería no funcional, imposibilidad de vinculación o cualquier condición que comprometa la continuidad, confiabilidad o seguridad del monitoreo.

La clasificación técnica deberá constar en el acta, informe, matriz o registro institucional correspondiente y servirá de sustento para la continuidad del uso, mantenimiento, sustitución, reposición, baja, custodia o demás acciones que correspondan conforme el procedimiento aplicable.

Artículo 90.- Acta o informe de soporte técnico. Toda atención de soporte técnico deberá constar en un acta, informe o registro institucional que contenga, al menos:

a. Datos de identificación del usuario;
b. Número de causa o proceso judicial;
c. Autoridad judicial competente;

d. Número de serie o identificación del dispositivo;
e. Modalidad de vigilancia electrónica;
f. Fecha, hora y lugar de atención;
g. Nombre del técnico responsable;
h. Descripción de la novedad reportada;
i. Diagnóstico técnico realizado;
j. Acción ejecutada;
k. Resultado de la atención;
l. Recomendaciones técnicas, cuando correspondan;
m. Firma del técnico, usuario y demás intervinientes, cuando aplique; y,
n. Anexos fotográficos o respaldos documentales.

Artículo 91.- Sustitución, reposición o cambio del Dispositivo de Vigilancia Electrónica.
La sustitución, reposición o cambio del Dispositivo de Vigilancia Electrónica procederá cuando el diagnóstico técnico determine que el equipo no se encuentra en condiciones adecuadas de funcionamiento, presenta falla permanente de orden técnico, daño físico, manipulación, corte, deterioro, pérdida de funcionalidad, incompatibilidad con la plataforma institucional, necesidad de actualización tecnológica, mantenimiento, renovación operativa o cualquier otra condición que comprometa la continuidad, confiabilidad o seguridad del monitoreo.

Cuando el equipo técnico detecte una falla permanente de orden técnico del Dispositivo de Vigilancia Electrónica, o cuando por razones técnicas, operativas, tecnológicas, logísticas o de seguridad resulte necesario mantener la prestación del servicio y precautelar el cumplimiento de la medida judicial, el cambio o reemplazo del dispositivo podrá ser dispuesto por la o el servidor encargado de la Gestión de Dispositivos de Vigilancia Electrónica de la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, o quien haga sus veces, sobre la base del informe, diagnóstico técnico, reporte de novedad o registro institucional correspondiente.

La sustitución, reposición o cambio deberá ejecutarse de manera documentada y trazable, verificando la identidad de la persona monitoreada, retirando el dispositivo anterior, instalando el nuevo equipo, actualizando la información en la Plataforma del Sistema de Vigilancia Electrónica, registrando el número de serie del dispositivo retirado y del nuevo dispositivo, validando la transmisión de señal y dejando constancia en el acta o informe correspondiente.

La sustitución, reposición o cambio deberá ser registrada en la plataforma institucional, incorporando los datos de vinculación, parámetros de monitoreo, acta correspondiente, diagnóstico técnico, disposición interna y demás respaldos al expediente físico o digital de la persona monitoreada.

El cambio del dispositivo no modificará por sí mismo las condiciones impuestas por la autoridad judicial competente ni suspenderá el monitoreo, debiendo garantizarse la continuidad del control electrónico durante el procedimiento. Una vez ejecutado el cambio o reemplazo, se notificará a la autoridad jurisdiccional competente, cuando corresponda.

Artículo 92.- Registro de dispositivos retirados, sustituidos o dañados. Los dispositivos retirados, sustituidos, reemplazados o identificados como dañados deberán ser registrados en la matriz o sistema institucional correspondiente, indicando su estado, motivo del retiro, diagnóstico técnico, usuario al que se encontraba asignado, número de serie, fecha de retiro, técnico responsable y destino del equipo.

La unidad responsable deberá garantizar la custodia, trazabilidad y control de los equipos retirados, conforme los procedimientos institucionales y patrimoniales aplicables.

Artículo 93.- Desinstalación del Dispositivo de Vigilancia Electrónica. La desinstalación del Dispositivo de Vigilancia Electrónica procederá únicamente cuando exista disposición judicial emitida por autoridad competente, o cuando la normativa vigente habilite su desactivación, retiro o desvinculación conforme el

procedimiento institucional aplicable.

La desinstalación deberá ejecutarse de manera documentada, segura y trazable, garantizando el registro del retiro físico del dispositivo, desvinculación en plataforma, cierre del monitoreo y comunicación a la autoridad competente.

Artículo 94.- Desinstalación en modalidad de libre circulación. En los casos de libre circulación, recibida la disposición judicial de desinstalación, la unidad responsable coordinará con la persona portadora del dispositivo su comparecencia al punto autorizado del SNAI para ejecutar el retiro del equipo.

El procedimiento deberá realizarse dentro del término establecido por la normativa vigente o por los procedimientos institucionales, dejando constancia de la fecha, hora, lugar, técnico responsable, número de serie del dispositivo retirado, estado del equipo y demás respaldos correspondientes.

Artículo 95.- Desinstalación en modalidad de arresto domiciliario. En los casos de arresto domiciliario, recibida la disposición judicial de desinstalación, la unidad responsable coordinará la logística necesaria para que el técnico asignado acuda al domicilio correspondiente o al lugar autorizado por la autoridad competente, a fin de ejecutar el retiro del Dispositivo de Vigilancia Electrónica.

El técnico deberá levantar el acta o informe respectivo, registrar la georreferenciación de la visita cuando sea posible, incorporar anexo fotográfico y remitir los documentos de respaldo a la unidad responsable.

Artículo 96.- Desvinculación en plataforma. Luego del retiro físico del Dispositivo de Vigilancia Electrónica, el operador de plataforma o servidor autorizado deberá ejecutar la desvinculación del equipo en la Plataforma del Sistema de Vigilancia Electrónica, dejando constancia del cierre del monitoreo, fecha y hora de desvinculación, responsable de la acción y estado final del dispositivo.

La desvinculación deberá realizarse únicamente respecto de casos en los cuales exista respaldo documental suficiente que habilite el cierre del monitoreo.

El cierre documental del monitoreo y el registro de la actuación se coordinarán con la desinstalación física prevista en el artículo 93 del presente Reglamento Técnico, cuando corresponda.

Artículo 97.- Acta de desinstalación. Toda desinstalación del Dispositivo de Vigilancia Electrónica deberá contar con un acta o informe institucional que contenga, al menos:

a. Datos de identificación del usuario;
b. Número de causa o proceso judicial;
c. Autoridad judicial competente;
d. Modalidad de vigilancia electrónica;
e. Número de serie del dispositivo retirado;
f. Fecha, hora y lugar de desinstalación;
g. Estado físico y funcional del dispositivo al momento del retiro;
h. Nombre del técnico responsable;
i. Registro de desvinculación en plataforma;
j. Observaciones o novedades identificadas;
k. Firma del usuario, técnico y demás intervinientes, cuando corresponda; y,
l. Anexos fotográficos o documentales de respaldo.

Artículo 98.- No comparecencia para desinstalación. Cuando la persona portadora del DVE no comparezca al punto autorizado para la desinstalación, no permita el retiro del dispositivo o no pueda ser ubicada, la unidad responsable deberá dejar constancia de la novedad y comunicarla a la autoridad judicial competente, adjuntando los respaldos respectivos.

En estos casos, el monitoreo se mantendrá activo hasta que exista disposición judicial o actuación administrativa habilitante para el cierre correspondiente, conforme la normativa aplicable.

Artículo 99.- Dispositivo no recuperado. Cuando el Dispositivo de Vigilancia Electrónica no pueda ser recuperado por pérdida, abandono, ocultamiento, negativa de entrega, corte, retiro no autorizado o cualquier otra circunstancia atribuible al usuario o a terceros, la unidad responsable deberá registrar la novedad, elaborar el informe correspondiente y poner el hecho en conocimiento de la autoridad competente.

La activación de procedimientos administrativos, patrimoniales o legales se realizará conforme la regulación prevista para los daños atribuibles al usuario o a terceros, establecida en el artículo 111 del presente Reglamento Técnico, en lo que fuere aplicable.

Artículo 100.- Estado del dispositivo al momento del retiro. El técnico responsable deberá verificar y registrar el estado físico y funcional del Dispositivo de Vigilancia Electrónica al momento del retiro, identificando si el equipo se encuentra operativo, deteriorado, dañado, manipulado, cortado, incompleto, descargado, sin accesorios o con cualquier novedad relevante.

Cuando se identifique daño, manipulación, corte, pérdida de componentes o deterioro no atribuible al uso normal, se deberá activar el procedimiento correspondiente para la gestión de dispositivos dañados y determinación de responsabilidades.

Artículo 101.- Comunicación de desinstalación a la autoridad judicial. Ejecutada la desinstalación, desvinculación y cierre del monitoreo, la unidad responsable comunicará a la autoridad judicial competente el cumplimiento de la disposición, conforme a las reglas de comunicación previstas en el Capítulo XI del presente Reglamento.

Para tal efecto, se adjuntará el acta de desinstalación prevista en el artículo 97 del presente Reglamento Técnico, junto con los respaldos que correspondan.

Artículo 102.- Responsabilidad por omisión en soporte o desinstalación. La falta de atención oportuna de requerimientos de soporte técnico, la omisión de registro, la desinstalación sin respaldo documental, la desvinculación indebida en plataforma, la pérdida de trazabilidad del dispositivo o la falta de comunicación a la autoridad competente podrán generar responsabilidades administrativas, civiles o penales, conforme la normativa vigente.

CAPÍTULO VIII

DE LA GESTIÓN DE DISPOSITIVOS DE VIGILANCIA ELECTRÓNICA DAÑADOS

Artículo 103.- Gestión de Dispositivos de Vigilancia Electrónica dañados. La gestión de Dispositivos de Vigilancia Electrónica dañados comprende las acciones de identificación, reporte, diagnóstico, registro, custodia, reparación, sustitución, reposición, control y cierre de casos relacionados con equipos que presenten daño físico, falla técnica, deterioro, manipulación, corte, alteración, pérdida de funcionalidad o cualquier otra condición que afecte su operación normal.

Artículo 104.- Identificación del daño. El daño del Dispositivo de Vigilancia Electrónica podrá ser identificado por el personal de monitoreo, soporte técnico, técnico de instalación, supervisor, usuario portador del dispositivo, autoridad competente o cualquier servidor que, en el ejercicio de sus funciones, advierta una novedad que afecte el estado físico o funcional del equipo.

Toda identificación de daño deberá ser registrada y comunicada a la unidad responsable para la atención correspondiente.

Artículo 105.- Reporte de novedad por daño. Cuando se identifique o presuma daño en un Dispositivo de Vigilancia Electrónica, se deberá generar el reporte de novedad correspondiente, en el que conste, al menos:

a. Datos de identificación del usuario;
b. Número de causa o proceso judicial;
c. Número de serie del dispositivo;
d. Modalidad de vigilancia electrónica;
e. Fecha, hora y lugar de identificación de la novedad;
f. Descripción del daño, falla o novedad;
g. Responsable que reporta el evento;
h. Acciones iniciales ejecutadas; y,
i. Evidencia o respaldo disponible.

Artículo 106.- Clasificación de la causa del daño. El personal técnico asignado realizará la verificación técnica del dispositivo reportado como dañado se efectuará conforme el procedimiento general de diagnóstico técnico previsto en el artículo 89 del presente Reglamento Técnico.

Con base en dicho diagnóstico, el personal técnico deberá clasificar la causa del daño como falla técnica, desgaste por uso normal, defecto del equipo, manipulación, corte, golpe, alteración, uso inadecuado, pérdida de componentes u otra causa verificable, dejando constancia de los respaldos correspondientes.

Artículo 107.- Clasificación del daño. Para efectos de control y gestión institucional, los daños de los Dispositivos de Vigilancia Electrónica podrán clasificarse de manera general en:

a. Daño técnico o falla operativa: aquel producido por defectos del equipo, fallas del sistema, problemas de batería, conectividad, transmisión, sensores o componentes internos;
b. Daño por desgaste o uso normal: aquel derivado del uso ordinario del dispositivo, siempre que no existan indicios de manipulación, mal uso o intervención indebida;
c. Daño por manipulación o uso indebido: aquel generado por corte, apertura, golpe, alteración, intervención no autorizada, exposición a condiciones no permitidas, desconexión, bloqueo, retiro o cualquier acción atribuible al usuario o a terceros; y,
d. Daño no determinado: aquel respecto del cual no sea posible establecer inicialmente la causa, hasta que se cuente con mayor análisis técnico o documentación de respaldo.

Artículo 108.- Medidas inmediatas frente a dispositivo dañado. Cuando el daño del dispositivo comprometa la continuidad del monitoreo, la transmisión de señal, la integridad del equipo o el cumplimiento de la disposición judicial, la unidad responsable deberá adoptar medidas inmediatas para garantizar el control del usuario monitoreado.

Estas medidas podrán incluir contacto con el usuario, seguimiento en tiempo real, soporte técnico, sustitución del dispositivo, escalamiento al supervisor, coordinación con autoridad competente o comunicación a la autoridad judicial, según la criticidad del caso.

Artículo 109.- Custodia del dispositivo dañado. El dispositivo dañado retirado deberá ser registrado, etiquetado, custodiado y almacenado conforme los procedimientos institucionales, garantizando su trazabilidad desde el retiro hasta su diagnóstico final, reparación, baja, devolución, reposición o destino que corresponda.

La custodia del equipo deberá prevenir pérdida, manipulación, alteración de evidencia, confusión de números de serie o uso no autorizado.

Artículo 110.- Reparación del dispositivo. Cuando el diagnóstico técnico determine que el dispositivo dañado puede ser reparado, la unidad responsable gestionará la reparación conforme los procedimientos internos, garantías, contratos, disponibilidad de repuestos, soporte del proveedor o mecanismos institucionales

aplicables.

El equipo reparado no podrá ser reasignado hasta que se verifique su funcionamiento, transmisión, integridad, seguridad y correcta operación en la plataforma institucional.

Artículo 111.- Daño atribuible al usuario o a terceros. Cuando del diagnóstico técnico, informe, alerta, evidencia fotográfica, reporte de monitoreo o demás respaldos se desprenda que el daño del Dispositivo de Vigilancia Electrónica podría ser atribuible al usuario o a terceros, la unidad responsable deberá elaborar el informe correspondiente y poner la novedad en conocimiento de la autoridad competente.

Sin perjuicio de la comunicación a la autoridad judicial, se activarán los procedimientos administrativos, patrimoniales o legales que correspondan para la determinación de responsabilidades y recuperación del bien o valor respectivo.

Artículo 112.- Daño no atribuible al usuario. Cuando el daño corresponda a falla técnica, desgaste por uso normal, defecto del equipo o circunstancias no atribuibles al usuario, la unidad responsable gestionará el soporte, reparación o sustitución correspondiente, procurando garantizar la continuidad del monitoreo y evitando afectaciones injustificadas al usuario.

Dicha condición deberá constar en el diagnóstico técnico o informe respectivo.

Artículo 113.- Dispositivo inutilizado o no recuperable. Cuando el dispositivo se encuentre inutilizado, irreparable, incompleto, perdido, cortado, alterado o en condiciones que impidan su reutilización, la unidad responsable deberá registrar tal condición y remitir la información a las áreas competentes para las acciones administrativas, patrimoniales, contractuales o legales que correspondan.

El estado de inutilización o no recuperación deberá estar sustentado en informe técnico y respaldos documentales o fotográficos.

Artículo 114.- Comunicación a la autoridad judicial por daño del dispositivo. Cuando el daño del dispositivo pueda afectar el cumplimiento de la disposición judicial, evidencie manipulación, corte, alteración, pérdida del equipo, retiro no autorizado o cualquier posible incumplimiento, la unidad responsable comunicará la novedad a la autoridad judicial competente cumpliendo con todos los parámetros establecidos en el Capítulo XI del presente Reglamento Técnico.

Artículo 115.- Informe técnico por dispositivo dañado. El informe deberá contener únicamente los elementos propios del análisis técnico posterior al reporte inicial, entre ellos:

a. Antecedentes del caso;
b. Diagnóstico técnico;
c. Clasificación del daño;
d. Evidencia fotográfica, documental o tecnológica relevante;
e. Acciones ejecutadas;
f. Estado final del dispositivo;
g. Conclusiones técnicas; y,
h. Recomendaciones.

Artículo 116.- Seguimiento y cierre del caso. Todo caso relacionado con un Dispositivo de Vigilancia Electrónica dañado deberá contar con seguimiento hasta su cierre, el cual procederá cuando se haya ejecutado la sustitución, reparación, comunicación a la autoridad competente, registro patrimonial, determinación de destino del equipo o cualquier otra acción que corresponda.

El cierre deberá constar en la matriz, sistema, expediente o informe respectivo.

Artículo 117.- Responsabilidad por omisión en la gestión de dispositivos dañados. La falta de reporte, diagnóstico, registro, custodia, sustitución, comunicación, seguimiento o cierre de casos relacionados con Dispositivos de Vigilancia Electrónica dañados podrá generar responsabilidades administrativas, civiles o penales, conforme la normativa vigente.

CAPÍTULO IX

DEL PAGO, EXONERACIÓN, REDUCCIÓN Y DIFERIMIENTO DEL VALOR POR USO Y MANTENIMIENTO DEL DISPOSITIVO DE VIGILANCIA ELECTRÓNICA

Artículo 118.- Pago por uso y mantenimiento del Dispositivo de Vigilancia Electrónica. Una vez que la autoridad judicial competente disponga el uso del Dispositivo de Vigilancia Electrónica, la persona usuaria deberá realizar el pago del valor determinado por el SNAI por concepto de uso y mantenimiento del dispositivo, de conformidad con la tarifa aprobada y los procedimientos financieros institucionales aplicables.

El pago deberá efectuarse mediante depósito, transferencia bancaria u otro mecanismo de recaudación habilitado institucionalmente, en la cuenta o canal financiero que el SNAI determine para el efecto, conforme la información que sea comunicada oficialmente a la persona usuaria.

La persona usuaria contará con el término de un día hábil, contado desde la notificación o comunicación institucional correspondiente, para realizar el pago y remitir el comprobante respectivo por los canales institucionales definidos para el efecto, sin perjuicio de otros mecanismos de recepción, registro o validación que establezca el área competente.

El comprobante de pago remitido por la persona usuaria será puesto en conocimiento del área financiera competente, a fin de que se efectúe la verificación del ingreso, el registro correspondiente y la emisión de la factura, conforme los procedimientos financieros institucionales aplicables.

La instalación, activación o continuidad del procedimiento correspondiente estará sujeta a la confirmación del pago por parte del área financiera competente, sin perjuicio de los casos en que proceda la exoneración, reducción o diferimiento del pago conforme el presente Reglamento Técnico.

Artículo 119.- Anticipo por uso y mantenimiento del Dispositivo de Vigilancia Electrónica. Con la finalidad de garantizar la continuidad operativa del Servicio de Vigilancia Electrónica, el monitoreo permanente, el soporte tecnológico, la disponibilidad de la plataforma, la conectividad, el mantenimiento, la gestión administrativa y la capacidad de respuesta ante incidentes, la persona usuaria deberá cancelar, en calidad de anticipo, el valor correspondiente a seis meses de uso y mantenimiento del Dispositivo de Vigilancia Electrónica, calculado sobre la base de la tarifa mensual aprobada.

El anticipo constituye un mecanismo de previsión financiera y continuidad del servicio, orientado a asegurar que, desde el inicio de la instalación y activación del dispositivo, existan valores previamente cancelados para cubrir los costos asociados a la prestación del servicio, sin que ello implique el pago total del período de duración de la medida judicial.

El valor correspondiente al anticipo deberá ser cancelado previo a la instalación, activación o continuidad del procedimiento que corresponda, salvo que la persona usuaria cuente con resolución administrativa vigente de exoneración, reducción o diferimiento del pago, conforme las reglas previstas en el presente Reglamento Técnico.

Cuando la persona usuaria acredite encontrarse dentro de los parámetros establecidos para reducción, exoneración o diferimiento, el anticipo podrá ser reducido, exonerado o diferido, según corresponda, mediante resolución administrativa debidamente motivada.

La falta de pago del anticipo no habilitará por sí sola la desinstalación del Dispositivo de Vigilancia Electrónica, salvo disposición judicial o normativa expresa que lo permita; sin embargo, deberá registrarse la novedad y ponerse en conocimiento de la autoridad judicial competente, garantizando la continuidad del monitoreo mientras se mantenga vigente la disposición judicial.

Artículo 120.- Verificación financiera, emisión de factura y confirmación del pago. Recibido el comprobante de depósito, transferencia u otro mecanismo de pago remitido por la persona usuaria, el área financiera competente verificará que el pago corresponda al valor aplicable, anticipo, cuenta o canal institucional autorizado, concepto de pago y persona usuaria respecto de quien se dispuso el uso del Dispositivo de Vigilancia Electrónica.

La verificación del pago confirmado por el área financiera competente, o de la resolución administrativa vigente de exoneración, reducción o diferimiento, constituirá requisito previo para continuar con la instalación, activación o actuación que corresponda, conforme la disposición judicial y el procedimiento institucional aplicable.

La verificación financiera deberá realizarse conforme los procedimientos internos del área competente, una vez recibido el comprobante de pago por los canales institucionales establecidos para el efecto.

Una vez verificado el pago, el área financiera competente emitirá o gestionará la factura correspondiente y remitirá la confirmación del pago, junto con la factura o respaldo financiero pertinente, a la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, a través de la gestión de Dispositivos de Vigilancia Electrónica, para que se continúe con el procedimiento de instalación, activación o actuación que corresponda.

Cuando el pago no pueda ser verificado, sea incompleto, corresponda a una cuenta o canal no autorizado, no permita identificar a la persona usuaria o presente inconsistencias, el área financiera competente informará dicha novedad a la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, a través de la gestión de Dispositivos de Vigilancia Electrónica, a fin de que se solicite la subsanación correspondiente a la persona usuaria.

La confirmación del pago, factura, comprobante y demás respaldos financieros deberán incorporarse al expediente físico o digital correspondiente, garantizando la trazabilidad documental del procedimiento.

Artículo 121.- Solicitud de exoneración, reducción o diferimiento del pago. La persona usuaria podrá solicitar la exoneración, reducción o diferimiento del pago por concepto de uso y mantenimiento del Dispositivo de Vigilancia Electrónica, cuando considere que se encuentra dentro de los parámetros técnicos, socioeconómicos, familiares o de vulnerabilidad previstos en la normativa vigente y en los instrumentos institucionales aplicables.

La solicitud deberá presentarse por escrito ante la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, dentro del término de un día hábil contado desde la notificación de la disposición judicial, y deberá contener, al menos, la identificación de la persona solicitante, número de causa, autoridad judicial competente, modalidad de vigilancia electrónica, petición concreta de exoneración, reducción o diferimiento, exposición breve de la situación alegada y documentación de respaldo.

La Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción receptará la solicitud, verificará la documentación presentada y continuará con el trámite correspondiente conforme los parámetros establecidos en el presente Reglamento Técnico y demás instrumentos institucionales aplicables.

La presentación de la solicitud no suspenderá por sí sola las obligaciones económicas generadas, salvo que exista resolución administrativa que así lo determine.

Artículo 122.- Documentación de respaldo. Para la evaluación de la solicitud de exoneración, reducción o diferimiento del pago, la persona usuaria deberá acompañar la documentación que permita verificar de manera objetiva la condición alegada, según corresponda.

Para el efecto, se considerarán, entre otros, los siguientes documentos de respaldo:

a. Persona adulta mayor: se verificará mediante la cédula de identidad, pasaporte u otro documento oficial que permita acreditar que la persona usuaria ha cumplido sesenta y cinco (65) años de edad.
b. Discapacidad: se verificará mediante el carné de discapacidad, certificado de discapacidad o documento emitido por la autoridad competente, en el cual conste el porcentaje de discapacidad reconocido.
c. Enfermedad catastrófica, rara, huérfana, grave o de alta complejidad: se verificará mediante certificado médico, informe médico, historia clínica, epicrisis o documentación emitida por la autoridad sanitaria competente o por el establecimiento de salud correspondiente, que permita acreditar dicha condición.
d. Sustituto directo de persona con discapacidad: se verificará mediante el certificado o documento emitido por el ente rector del trabajo o por la autoridad competente, en el cual conste dicha calidad.
e. Situación laboral e ingresos económicos: se verificará mediante mecanizado del IESS, certificado laboral, rol de pagos, contrato de trabajo, declaración de impuesto a la renta, RUC, RIMPE, certificación de no afiliación, declaración juramentada de ingresos, estados de cuenta u otros documentos que permitan determinar la capacidad económica real de la persona usuaria.
f. Cargas familiares o dependencia económica: se verificará mediante cédulas de identidad, partidas de nacimiento, certificado de matrimonio, declaración de unión de hecho, certificados de discapacidad de dependientes, certificados de estudio de hijos dependientes, declaración juramentada de dependencia económica u otros documentos que permitan acreditar que las personas señaladas dependen económicamente de la persona usuaria.
g. Capacidad real de pago: se verificará a partir del análisis conjunto de los ingresos, egresos básicos, situación laboral, cargas familiares, condiciones de vulnerabilidad y demás documentación incorporada al expediente administrativo.

La Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción podrá requerir la aclaración, complemento o actualización de la documentación presentada cuando esta sea incompleta, ilegible, inconsistente o insuficiente para resolver la solicitud, dejando constancia de dicha actuación en el expediente correspondiente.

Artículo 123.- Parámetros para la exoneración, reducción o diferimiento del pago. Para la evaluación de las solicitudes, la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción considerará de forma objetiva, proporcional y documentada los parámetros técnicos, socioeconómicos, familiares y de vulnerabilidad previstos en la normativa vigente, la tarifa aprobada y el presente Reglamento Técnico.

Para efectos de la aplicación de los beneficios de exoneración, reducción o diferimiento del pago, se observarán los siguientes parámetros:

a. Discapacidad de la persona usuaria: cuando la persona usuaria acredite un porcentaje de discapacidad comprendido entre el treinta por ciento (30%) y el ochenta y cuatro por ciento (84%), podrá acceder a una reducción equivalente al cincuenta por ciento (50%) de la tarifa asignada por uso y mantenimiento del Dispositivo de Vigilancia Electrónica. Cuando acredite un porcentaje de discapacidad igual o superior al ochenta y cinco por ciento (85%), podrá acceder a una exoneración equivalente al cien por ciento (100%) de la tarifa correspondiente.

b. Enfermedad catastrófica, rara, huérfana, grave o de alta complejidad: cuando la persona usuaria acredite dicha condición mediante certificado médico, informe médico o documentación emitida por la autoridad sanitaria competente o por el establecimiento de salud correspondiente, podrá acceder a una exoneración equivalente al cien por ciento (100%) de la tarifa asignada por uso y mantenimiento del Dispositivo de

Vigilancia Electrónica.

c. Sustituto directo de persona con discapacidad: cuando la persona usuaria acredite la calidad de sustituto directo de persona con discapacidad, podrá acceder a una reducción equivalente al cincuenta por ciento (50%) de la tarifa asignada por uso y mantenimiento del Dispositivo de Vigilancia Electrónica.

d. Persona adulta mayor: cuando la persona usuaria acredite haber cumplido sesenta y cinco (65) años de edad, podrá acceder a una reducción equivalente al cincuenta por ciento (50%) de la tarifa asignada por uso y mantenimiento del Dispositivo de Vigilancia Electrónica.

e. Factor económico-financiero: para la valoración del factor económico-financiero se tomará como referencia el nivel de ingresos mensuales de la persona usuaria. Se considerará que la persona usuaria que perciba ingresos superiores al equivalente a 3,45 salarios básicos unificados mensuales cuenta, en términos generales, con capacidad económica para asumir el pago total de la tarifa establecida por uso y mantenimiento del Dispositivo de Vigilancia Electrónica.

Cuando la persona usuaria acredite ingresos inferiores al equivalente a 3,45 salarios básicos unificados mensuales, y de la revisión documental se determine que no cuenta con liquidez inmediata para cubrir el valor exigible, pero mantiene capacidad parcial de pago, podrá acceder al diferimiento del pago, conforme el cronograma que se establezca en la resolución administrativa correspondiente.

La verificación de este factor se realizará mediante la revisión de la documentación económica presentada por la persona usuaria, tales como mecanizado del IESS, certificado laboral, roles de pago, contrato de trabajo, declaración de impuesto a la renta, RUC, RIMPE, certificado de no afiliación, declaración juramentada de ingresos, estados de cuenta u otros documentos que permitan determinar objetivamente sus ingresos y capacidad real de pago.

f. Factor familiar o cargas familiares: cuando la persona usuaria acredite la existencia de cargas familiares o dependencia económica de terceros que incidan en su capacidad de pago, podrá acceder al diferimiento del pago, conforme el análisis documentado que realice la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción.

g. Capacidad real de pago: la capacidad real de pago será valorada a partir del análisis conjunto de los ingresos, situación laboral, cargas familiares, condiciones de vulnerabilidad, obligaciones económicas básicas y demás documentación incorporada al expediente, con la finalidad de determinar la procedencia de la exoneración, reducción o diferimiento, según corresponda.

La reducción procederá respecto de los factores expresamente vinculados a discapacidad entre el treinta por ciento (30%) y el ochenta y cuatro por ciento (84%), calidad de sustituto directo de persona con discapacidad o condición de persona adulta mayor. La exoneración procederá respecto de discapacidad igual o superior al ochenta y cinco por ciento (85%) y enfermedad catastrófica, rara, huérfana, grave o de alta complejidad debidamente acreditada. El diferimiento procederá principalmente respecto de los factores económico-financieros y familiares o de cargas familiares, conforme el cronograma y condiciones que se establezcan en la resolución administrativa correspondiente.

Los porcentajes, condiciones, plazos y reglas específicas de aplicación se sujetarán a la tarifa aprobada y a los instrumentos institucionales que se emitan para el efecto.

Artículo 124.- Trámite de la solicitud. Recibida la solicitud de exoneración, reducción o diferimiento, la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción verificará la documentación presentada, analizará la procedencia de la petición y elaborará el informe técnico, económico, socioeconómico o administrativo correspondiente, según la naturaleza del caso.

El trámite deberá gestionarse, de manera referencial, dentro del término de tres días hábiles, distribuidos de la

siguiente manera:

a. Primer día hábil: recepción de la solicitud y verificación inicial de la documentación presentada;
b. Segundo día hábil: análisis de la información, validación de los factores aplicables y elaboración del informe correspondiente; y,
c. Tercer día hábil: emisión de la resolución administrativa que conceda o niegue la exoneración, reducción o diferimiento solicitado.

Cuando la complejidad del caso, la necesidad de validación con otras unidades o la falta de documentación suficiente impidan resolver dentro del término referencial señalado, la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción dejará constancia motivada en el expediente y continuará el trámite con la debida diligencia.

Artículo 125.- Resolución de exoneración, reducción o diferimiento. La exoneración, reducción o diferimiento del pago por uso y mantenimiento del Dispositivo de Vigilancia Electrónica deberá resolverse mediante acto administrativo debidamente motivado, emitido por la autoridad competente del SNAI o su delegado.

La resolución deberá determinar expresamente si se concede o niega la solicitud, el alcance de la exoneración, el porcentaje de reducción o las condiciones del diferimiento, el plazo de vigencia, las obligaciones de la persona usuaria, la forma de control y los demás aspectos necesarios para su ejecución.

La resolución deberá sustentarse en los parámetros previstos en el artículo 123 del presente Reglamento, en la documentación incorporada al expediente y en el informe técnico, económico, socioeconómico o administrativo correspondiente.

Artículo 126.- Diferimiento del pago. Cuando se conceda el diferimiento del pago, la resolución administrativa establecerá el valor inicial que deberá cancelar la persona usuaria, el cronograma de pagos, la periodicidad, el plazo máximo aplicable, la forma de pago y las consecuencias derivadas del incumplimiento.

El diferimiento se aplicará como un mecanismo administrativo que permite postergar o distribuir el cumplimiento de la obligación económica, sin que ello implique exoneración total del valor correspondiente, salvo que concurran otros factores debidamente justificados que permitan una reducción o exoneración, conforme la normativa vigente y los parámetros aplicables.

Para acceder al diferimiento, la persona usuaria deberá cancelar inicialmente el valor correspondiente a dos meses de uso y mantenimiento del Dispositivo de Vigilancia Electrónica, calculado sobre la base de la tarifa mensual aprobada. Dicho valor comprenderá el mes que inicia o se encuentra en curso y el mes inmediato siguiente, que será cancelado con carácter anticipado.

A partir del segundo pago, la persona usuaria deberá mantener el esquema de pago mensual anticipado, cancelando el valor correspondiente al mes inmediato siguiente, conforme el cronograma aprobado en la resolución administrativa correspondiente.

El diferimiento podrá concederse hasta por un plazo máximo de seis meses, mediante pagos mensuales anticipados, iguales y sucesivos, sin perjuicio de la revisión que corresponda en caso de incumplimiento, variación de las condiciones económicas o modificación de la medida judicial.

La falta de pago oportuno de una o más cuotas podrá dar lugar a la revisión, terminación o revocatoria del beneficio, sin perjuicio del registro de la novedad, la comunicación a la autoridad competente y las acciones administrativas que correspondan.

El diferimiento no exime a la persona usuaria del cumplimiento de las obligaciones derivadas del uso del Dispositivo de Vigilancia Electrónica, ni tendrá efecto retroactivo respecto de valores ya pagados.

Artículo 127.- Registro de pagos y resoluciones administrativas. Los pagos, comprobantes, anticipos, solicitudes, informes, resoluciones de exoneración, reducción o diferimiento, cronogramas y demás documentos relacionados con la obligación económica por uso y mantenimiento del Dispositivo de Vigilancia Electrónica deberán incorporarse al expediente físico o digital correspondiente.
La Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción mantendrá el registro y trazabilidad de dicha información, en coordinación con las áreas administrativas y financieras competentes, conforme los procedimientos institucionales aplicables.

Artículo 128.- Falta de pago. Cuando la persona usuaria no efectúe el pago o anticipo dentro del término previsto y no cuente con resolución administrativa vigente de exoneración, reducción o diferimiento, la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción registrará la novedad, realizará la verificación correspondiente y comunicará el hecho a la autoridad judicial competente, conforme el procedimiento institucional aplicable.

La falta de pago o anticipo no habilitará por sí sola la desinstalación del Dispositivo de Vigilancia Electrónica, salvo disposición judicial o normativa expresa que lo permita, debiendo garantizarse la continuidad del monitoreo mientras se mantenga vigente la disposición judicial.

Artículo 129.- Control y seguimiento de obligaciones de pago. La Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, en coordinación con las áreas administrativas y financieras competentes, implementará mecanismos de control y seguimiento de pagos, anticipos, exoneraciones, reducciones, diferimientos, valores pendientes, vencimientos, cronogramas y demás información relacionada con el uso y mantenimiento del Dispositivo de Vigilancia Electrónica.

Artículo 130.- Responsabilidad por omisión de control. La omisión en la verificación, registro, control, comunicación o seguimiento de pagos, anticipos, exoneraciones, reducciones o diferimientos podrá generar responsabilidades administrativas, civiles o penales, conforme la normativa vigente.

CAPÍTULO X

DEL REGISTRO, ARCHIVO, CUSTODIA Y SEGURIDAD DE LA INFORMACIÓN

Artículo 131.- Registro obligatorio de actuaciones. Todas las actuaciones administrativas, técnicas, operativas, financieras y documentales relacionadas con la gestión del Servicio de Vigilancia Electrónica deberán ser registradas de manera clara, completa, cronológica y verificable en la plataforma institucional, matrices, bitácoras, expedientes, informes, actas o formatos establecidos para el efecto.

El registro deberá permitir identificar el responsable de la actuación, fecha, hora, tipo de procedimiento, número de causa, usuario monitoreado, dispositivo asignado, acción ejecutada, resultado obtenido y documentos de respaldo.

Artículo 132.- Plazo para carga de expediente en plataforma. El personal responsable deberá cargar el expediente digital en la Plataforma del Sistema de Vigilancia Electrónica o en el repositorio institucional definido para el efecto, dentro del término establecido por la unidad responsable, contado a partir de la ejecución de la instalación.

El incumplimiento injustificado de esta obligación deberá ser reportado al responsable inmediato superior, sin perjuicio de las responsabilidades administrativas que correspondan.

Artículo 133.- Expediente físico y digital. Por cada persona monitoreada con Dispositivo de Vigilancia Electrónica se deberá conformar un expediente físico o digital, según corresponda, que permita conservar de

manera ordenada la documentación generada durante la vigencia de la medida, beneficio, régimen o disposición judicial.

El expediente podrá contener, entre otros documentos:

a. Disposición judicial que ordena el uso del DVE;
b. Documentos de identificación;
c. Acta de instalación y entrega-recepción;
d. Acuerdo de uso del dispositivo;
e. Comprobante de pago o resolución de exoneración, reducción o diferimiento, cuando corresponda;
f. Informe de factibilidad técnica;
g. Registro de activación, parametrización y geocercas;
h. Informes de monitoreo y novedades;
i. Actas o informes de soporte técnico;
j. Informes por alertas, alarmas o incumplimientos;
k. Actas de sustitución, reposición o desinstalación;
l. Anexos fotográficos;
m. Comunicaciones remitidas o recibidas de autoridad competente; y,
n. Los demás documentos que respalden la gestión del caso.

Artículo 134.- Custodia documental. La unidad responsable garantizará la custodia, conservación, integridad, disponibilidad y trazabilidad de los expedientes físicos y digitales relacionados con el Servicio de Vigilancia Electrónica.

Los documentos deberán mantenerse en archivos, repositorios, sistemas o plataformas institucionales autorizadas, evitando pérdida, alteración, eliminación no autorizada, deterioro, acceso indebido o uso no permitido de la información.

Artículo 135.- Trazabilidad de la información. La información generada en la gestión del Servicio de Vigilancia Electrónica deberá contar con trazabilidad suficiente para reconstruir las actuaciones realizadas desde la recepción de la disposición judicial hasta el cierre del caso.

La trazabilidad deberá permitir identificar, al menos, el ingreso de la disposición judicial, verificación, instalación, activación, parametrización, monitoreo, alertas, alarmas, soporte técnico, pagos, exoneraciones, dispositivos dañados, desinstalación, comunicaciones y archivo final.

Artículo 136.- Seguridad de la información. La información relacionada con el Servicio de Vigilancia Electrónica será administrada bajo criterios de seguridad, confidencialidad, necesidad institucional, integridad, disponibilidad, reserva, protección de datos personales y acceso restringido, considerando su naturaleza sensible y su vinculación con la seguridad penitenciaria, el cumplimiento de disposiciones judiciales y la operación del Sistema de Vigilancia Electrónica.

El acceso a la información estará limitado al personal autorizado y únicamente para el cumplimiento de funciones institucionales vinculadas con la gestión, control, seguimiento, monitoreo, soporte, supervisión, evaluación o archivo del servicio.

Artículo 137.- Información de acceso restringido. Tendrá acceso restringido la información relacionada con ubicación de personas monitoreadas, geocercas, rutas, horarios, restricciones judiciales, alertas, alarmas, novedades, datos personales, documentos judiciales, informes de monitoreo, configuraciones técnicas, credenciales, parámetros de plataforma, registros de comunicación y demás información que pueda comprometer la seguridad del Sistema de Vigilancia Electrónica o los derechos de las personas involucradas.

El acceso, uso o entrega de esta información deberá sujetarse a la normativa vigente, a los perfiles autorizados y a las finalidades institucionales correspondientes.

Artículo 138.- Carácter reservado de la documentación. La documentación, registros, expedientes, informes, matrices, anexos, reportes, comunicaciones, respaldos técnicos, registros de geolocalización, configuraciones, parámetros de monitoreo, geocercas, alertas, alarmas, novedades y demás información generada o administrada dentro del Servicio de Vigilancia Electrónica tendrá el carácter de información reservada, confidencial o de acceso restringido, según corresponda, en atención a su naturaleza sensible, operativa, técnica, judicial, penitenciaria y de seguridad institucional.

La reserva de la información se fundamenta en la necesidad de proteger la seguridad del Sistema de Vigilancia Electrónica, la integridad de las personas monitoreadas, la eficacia del control dispuesto por autoridad competente, la seguridad penitenciaria, la protección de datos personales y la prevención de riesgos operativos o institucionales.

El acceso a dicha documentación estará limitado exclusivamente a los servidores públicos, autoridades judiciales, autoridades administrativas o instituciones competentes que, en el marco de sus atribuciones legales, requieran conocerla para fines estrictamente institucionales, judiciales, administrativos, técnicos, operativos o de control.

La entrega, reproducción, remisión o acceso a documentación relacionada con el Servicio de Vigilancia Electrónica deberá realizarse únicamente por canales oficiales, previa verificación de competencia, necesidad institucional y cumplimiento de la normativa aplicable sobre reserva, confidencialidad, protección de datos personales y seguridad de la información.

El personal de monitoreo deberá observar esta reserva respecto de datos personales, ubicación, geocercas, rutas, alertas, alarmas, condiciones judiciales, comunicaciones y demás información relacionada con las personas monitoreadas.

Artículo 139.- Prohibición de uso no autorizado de información reservada. Queda prohibido divulgar, reproducir, capturar, fotografiar, grabar, copiar, extraer, descargar, remitir, publicar, compartir o utilizar información reservada, confidencial o de acceso restringido del Servicio de Vigilancia Electrónica para fines ajenos a las competencias institucionales.

La prohibición incluye información contenida en plataformas, bitácoras, matrices, expedientes, informes, anexos fotográficos, comunicaciones, registros de geolocalización, datos personales, documentación judicial, parámetros técnicos, geocercas, alertas, alarmas, novedades operativas o cualquier otro soporte físico o digital.

Artículo 140.- Confidencialidad del procedimiento técnico. Durante la colocación física, revisión, configuración, activación o soporte del Dispositivo de Vigilancia Electrónica, el personal responsable deberá adoptar medidas que permitan preservar la confidencialidad del procedimiento técnico, la seguridad del dispositivo, la integridad del sistema y la reserva de la información operacional.

La confidencialidad del procedimiento técnico se aplicará como regla transversal de seguridad de la información, sin perjuicio de las medidas operativas específicas que deban adoptarse durante la instalación, activación, configuración, monitoreo o soporte del Dispositivo de Vigilancia Electrónica.

Artículo 141.- Restricción del uso de dispositivos personales. Se restringe el uso de teléfonos celulares personales, cámaras, dispositivos de grabación o cualquier otro medio tecnológico no autorizado durante los procedimientos de instalación, activación, soporte técnico, monitoreo, parametrización o gestión operativa del Sistema de Vigilancia Electrónica, especialmente cuando su uso pueda comprometer información sensible, datos personales, seguridad operativa o reserva institucional.

El uso de equipos tecnológicos institucionales deberá realizarse únicamente para fines relacionados con la ejecución del servicio y conforme los lineamientos internos de seguridad de la información.

Artículo 142.- Acceso a la plataforma institucional. El acceso a la Plataforma del Sistema de Vigilancia Electrónica deberá realizarse mediante credenciales institucionales, perfiles autorizados y mecanismos de control definidos por la unidad competente.

Artículo 143.- Responsabilidad sobre registros en plataforma. Todo servidor o personal autorizado será responsable de la veracidad, integridad y oportunidad de la información que registre en la plataforma institucional, bitácoras, matrices, expedientes o sistemas relacionados con el Servicio de Vigilancia Electrónica.

Los registros deberán efectuarse sin alteraciones, omisiones injustificadas, duplicidades, datos falsos, cierres indebidos o modificaciones no autorizadas.

Artículo 144.- Respaldo de documentos y evidencias. Los documentos, reportes, capturas, registros, anexos fotográficos, informes, actas, comprobantes y demás evidencias generadas dentro del Servicio de Vigilancia Electrónica deberán respaldarse en los repositorios institucionales definidos para el efecto.

El respaldo de documentos deberá realizarse dentro de los plazos establecidos por la unidad responsable y bajo criterios de organización, identificación, seguridad, reserva y disponibilidad.

Artículo 145.- Archivo de comunicaciones judiciales. Toda comunicación remitida o recibida de autoridad judicial competente deberá incorporarse al expediente físico o digital de la persona monitoreada, junto con los respaldos que motivaron dicha comunicación.

Cuando se trate de novedades, incumplimientos, alertas críticas, daños, desinstalaciones, falta de pago, no comparecencia o imposibilidad de cumplimiento, deberá conservarse el informe o documento técnico que sustente la comunicación realizada.

Artículo 146.- Integridad de expedientes. Los expedientes del Servicio de Vigilancia Electrónica deberán mantenerse íntegros, ordenados y actualizados. La incorporación, retiro, modificación o eliminación de documentos deberá realizarse únicamente conforme los procedimientos institucionales autorizados.

Cualquier pérdida, alteración, extracción o manipulación no autorizada de documentos deberá ser reportada de manera inmediata al responsable superior, sin perjuicio de las acciones administrativas o legales que correspondan.

Artículo 147.- Interoperabilidad y uso de sistemas institucionales. Cuando existan sistemas, plataformas o herramientas tecnológicas interoperables relacionadas con la gestión penitenciaria, vigilancia electrónica, archivo, seguimiento judicial, pagos, soporte técnico o monitoreo, la unidad responsable deberá procurar el uso articulado de dichos sistemas, conforme las competencias institucionales y disponibilidad tecnológica.

El uso de herramientas tecnológicas deberá garantizar la seguridad, trazabilidad, reserva y protección de la información.

Artículo 148.- Confidencialidad del personal interviniente. Los servidores públicos, personal técnico, operadores, supervisores y demás personas que intervengan en la gestión del Servicio de Vigilancia Electrónica estarán obligados a guardar confidencialidad respecto de la información conocida en razón de sus funciones.

La obligación de confidencialidad se mantendrá incluso después de haber cesado la relación laboral, contractual, funcional o institucional con el SNAI.

Artículo 149.- Responsabilidad por mal uso de información. El acceso, divulgación, modificación, eliminación, reproducción, extracción, entrega o uso no autorizado de información relacionada con el Servicio de Vigilancia Electrónica podrá generar responsabilidades administrativas, civiles o penales, conforme la normativa vigente.

Resolución Nro. SNAI-SNAI-2026-0052-R

Quito, D.M., 15 de mayo de 2026

CAPÍTULO XI

DE LA COORDINACIÓN INTERINSTITUCIONAL Y COMUNICACIONES CON AUTORIDAD COMPETENTE

Artículo 150.- Coordinación interinstitucional. La gestión del Servicio de Vigilancia Electrónica podrá requerir coordinación con autoridades judiciales, Fiscalía General del Estado, Policía Nacional, ECU 911, entidades de salud, unidades administrativas internas del SNAI u otras instituciones públicas competentes, conforme la naturaleza del caso, el nivel de criticidad del evento y las disposiciones judiciales aplicables.

La coordinación interinstitucional deberá realizarse de manera oportuna, documentada y por canales oficiales, garantizando la trazabilidad de las actuaciones ejecutadas.

Artículo 151.- Finalidad de la coordinación. La coordinación interinstitucional tendrá como finalidad garantizar el cumplimiento de las disposiciones judiciales, la atención oportuna de eventos críticos, la continuidad del monitoreo, la seguridad del usuario monitoreado, la recuperación o revisión del dispositivo, la atención de emergencias, la comunicación de incumplimientos y el seguimiento de novedades que requieran intervención de otras instituciones.

Artículo 152.- Comunicación con autoridad judicial competente. La unidad responsable deberá comunicar a la autoridad judicial competente las actuaciones, novedades o circunstancias relevantes relacionadas con el uso del Dispositivo de Vigilancia Electrónica, cuando corresponda.

Entre otros casos, se comunicará a la autoridad judicial competente:

a. Instalación y activación del DVE;
b. Imposibilidad de instalación;
c. No comparecencia del usuario para instalación, soporte o desinstalación;
d. Errores, inconsistencias u omisiones en la disposición judicial;
e. No factibilidad técnica de instalación;
f. Alertas o alarmas críticas;
g. Posibles incumplimientos de la disposición judicial;
h. Corte, manipulación, daño, pérdida o retiro no autorizado del dispositivo;
i. Pérdida prolongada de señal sin justificación o sin respuesta del usuario;
j. Desinstalación y desvinculación del dispositivo;
k. Falta de pago por concepto de uso y mantenimiento del DVE, cuando corresponda;
l. Necesidad de aclaración, ampliación o modificación de condiciones judiciales; y,
m. Cualquier otra novedad que pueda afectar el cumplimiento de la disposición judicial.

Artículo 153.- Contenido mínimo de las comunicaciones. Las comunicaciones oficiales relacionadas con el Servicio de Vigilancia Electrónica deberán contener, al menos:

a. Identificación de la autoridad o institución destinataria;
b. Número de causa o proceso judicial;
c. Datos de identificación de la persona monitoreada;
d. Modalidad de vigilancia electrónica;
e. Número de serie del dispositivo, cuando corresponda;
f. Antecedentes relevantes;
g. Descripción clara de la actuación, novedad o evento;
h. Fecha y hora de ocurrencia, atención o gestión;
i. Acciones ejecutadas por la unidad responsable;
j. Resultado obtenido o estado actual del caso;
k. Solicitud, recomendación o puesta en conocimiento, según corresponda; y,

l. Anexos, informes, actas, registros o respaldos documentales pertinentes.

Artículo 154.- Comunicación de imposibilidad de instalación. Cuando no sea posible ejecutar la instalación del Dispositivo de Vigilancia Electrónica por errores en la disposición judicial, ausencia del usuario, dirección incorrecta, falta de condiciones técnicas, imposibilidad de acceso, no comparecencia, falta de disponibilidad operativa u otra causa justificada, la unidad responsable comunicará dicha novedad a la autoridad judicial competente.

La comunicación deberá estar respaldada en informe técnico, acta, registro de gestión, anexo fotográfico o cualquier otro documento que permita justificar la imposibilidad de ejecución.

Artículo 155.- Comunicación de incumplimientos. Cuando del monitoreo, soporte técnico, atención de alertas, alarmas, reportes institucionales o demás actuaciones relacionadas con el Servicio de Vigilancia Electrónica se identifique un posible incumplimiento de la disposición judicial, la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, a través de la gestión de Dispositivos de Vigilancia Electrónica, comunicará la novedad a la autoridad judicial competente.

La comunicación deberá realizarse sin sustituir la valoración jurisdiccional de la autoridad competente, limitándose a informar de manera objetiva los hechos identificados, registros generados por el sistema, eventos, fechas, horarios, acciones ejecutadas, comunicaciones realizadas y respaldos disponibles.

De igual manera, cuando se verifique el incumplimiento del pago, anticipo o de las condiciones establecidas en la resolución administrativa de exoneración, reducción o diferimiento por concepto de uso y mantenimiento del Dispositivo de Vigilancia Electrónica, la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, a través de la gestión de Dispositivos de Vigilancia Electrónica, comunicará dicha novedad a la autoridad judicial competente, adjuntando los respaldos administrativos y financieros correspondientes, a fin de que dicha autoridad adopte las decisiones que estime pertinentes dentro del ámbito de sus competencias.

Artículo 156.- Comunicación de alertas críticas o eventos relevantes. Las alertas críticas o eventos relevantes que puedan comprometer el cumplimiento de la disposición judicial, la continuidad del monitoreo, la integridad del dispositivo o el control del usuario monitoreado deberán ser comunicados a la autoridad competente, cuando corresponda.
El catálogo de alertas críticas y eventos relevantes será el previsto en el artículo 57 del presente Reglamento Técnico, sin perjuicio de la valoración técnica y operativa que corresponda en cada caso.

Artículo 157.- Coordinación con Policía Nacional. Cuando un evento generado por el Sistema de Vigilancia Electrónica requiera intervención operativa, verificación territorial, apoyo de seguridad, localización del usuario, atención de posible incumplimiento, recuperación de dispositivo o respuesta frente a situaciones de riesgo, la unidad responsable podrá coordinar con la Policía Nacional, conforme los protocolos institucionales y competencias aplicables.

La coordinación deberá registrarse indicando fecha, hora, unidad policial contactada, responsable de la comunicación, acción solicitada, respuesta recibida y resultado obtenido.

Artículo 158.- Coordinación con ECU 911. Cuando la naturaleza del evento, alerta, alarma, emergencia o incidente lo requiera, la unidad responsable podrá coordinar con el ECU 911 para la atención o articulación correspondiente, de conformidad con los convenios, protocolos o mecanismos institucionales aplicables.
En estos casos deberá dejarse constancia del número de ficha, ticket, registro, hora de comunicación, servidor responsable, institución derivada y resultado de la gestión.

Artículo 159.- Coordinación con Fiscalía General del Estado. Cuando los hechos identificados puedan constituir indicios de infracción penal, incumplimiento de decisiones legítimas de autoridad competente, daño a bienes públicos, manipulación dolosa, pérdida intencional del dispositivo u otros hechos que deban ser

conocidos por Fiscalía, la unidad responsable podrá poner la novedad en conocimiento de la Fiscalía General del Estado, conforme los canales institucionales correspondientes.

La comunicación deberá acompañarse de los informes, actas, respaldos técnicos, registros de plataforma, anexos fotográficos y demás documentación pertinente.

Artículo 160.- Coordinación con entidades de salud. Cuando la persona monitoreada reporte una emergencia médica, urgencia, enfermedad grave, accidente, condición de salud que afecte el uso del DVE o imposibilidad temporal de cumplir determinadas condiciones por razones médicas, la unidad responsable podrá coordinar con las entidades de salud competentes, cuando corresponda.
La coordinación deberá registrarse y, de ser pertinente, comunicarse a la autoridad judicial competente para los fines correspondientes.

Artículo 161.- Coordinación interna del SNAI. La Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción coordinará con las unidades administrativas, financieras, jurídicas, tecnológicas, territoriales, de planificación, seguridad penitenciaria y demás áreas del SNAI que resulten necesarias para la adecuada gestión del Servicio de Vigilancia Electrónica.
La coordinación interna podrá comprender aspectos relacionados con disponibilidad de dispositivos, soporte tecnológico, pagos, exoneraciones, control patrimonial, desarrollo de procesos, archivo, seguridad de la información, contratación, mantenimiento, informes jurídicos o administrativos y demás acciones necesarias para el funcionamiento del servicio.

Artículo 162.- Uso de canales oficiales. Las comunicaciones y coordinaciones relacionadas con el Servicio de Vigilancia Electrónica deberán realizarse mediante canales oficiales, tales como sistemas documentales institucionales, correos electrónicos institucionales, oficios, memorandos, plataformas autorizadas, líneas oficiales de coordinación o cualquier otro medio institucionalmente habilitado.

Cuando por la urgencia del caso se utilicen medios inmediatos de comunicación, deberá dejarse constancia posterior en la bitácora, informe, matriz, sistema o expediente correspondiente.

Artículo 163.- Registro de coordinaciones. Toda coordinación interna o externa deberá ser registrada por el servidor responsable, indicando fecha, hora, institución o unidad contactada, persona o cargo con quien se coordinó, medio utilizado, motivo de la coordinación, acción solicitada, respuesta recibida, resultado obtenido y documentos de respaldo.

El registro de coordinación deberá incorporarse al expediente del caso cuando tenga relación directa con una persona monitoreada o con un evento específico.

Artículo 164.- Remisión de respaldos documentales. Cuando se remitan informes, actas, registros de plataforma, anexos fotográficos, capturas, matrices o cualquier otro respaldo documental a autoridad judicial o institución competente, deberá verificarse que la documentación sea pertinente, necesaria, íntegra y relacionada con el objeto de la comunicación.

La remisión deberá observar las disposiciones sobre reserva, confidencialidad, protección de datos personales y seguridad de la información.

Artículo 165.- Solicitudes de información. Las solicitudes de información relacionadas con el Servicio de Vigilancia Electrónica deberán ser atendidas conforme la competencia del requirente, la naturaleza de la información solicitada, el carácter reservado o restringido de la documentación y la normativa vigente.

Cuando la solicitud provenga de autoridad judicial, Fiscalía General del Estado u otra autoridad competente, la unidad responsable deberá preparar la respuesta institucional con los respaldos que correspondan, observando los principios de legalidad, oportunidad, reserva y trazabilidad.

Artículo 166.- Limitación en la entrega de información sensible. La entrega de información sensible, técnica, operativa, reservada o de acceso restringido del Servicio de Vigilancia Electrónica deberá limitarse a lo estrictamente necesario para atender el requerimiento formulado por autoridad competente.

No se entregará información que pueda comprometer la seguridad del Sistema de Vigilancia Electrónica, la integridad de las personas monitoreadas, la operación del centro de monitoreo, los parámetros técnicos del sistema o la eficacia de las medidas dispuestas, salvo requerimiento expreso de autoridad competente y conforme la normativa aplicable.

Artículo 167.- Responsabilidad en las comunicaciones. Los servidores responsables de elaborar, revisar, suscribir, remitir o registrar comunicaciones relacionadas con el Servicio de Vigilancia Electrónica deberán verificar la exactitud, pertinencia, reserva, integridad y suficiencia de la información incorporada.

Artículo 168.- Seguimiento de requerimientos externos. Los requerimientos formulados por autoridades judiciales, Fiscalía General del Estado, Policía Nacional, ECU 911 u otras instituciones competentes deberán ser objeto de seguimiento hasta su atención, cierre o archivo.
La unidad responsable deberá mantener un registro actualizado del estado de los requerimientos, fechas de ingreso, responsables asignados, plazo de atención, documentación remitida y resultado final.

CAPÍTULO XII

DE LA SUPERVISIÓN, RESPONSABILIDADES Y MEJORA CONTINUA DEL SERVICIO DE VIGILANCIA ELECTRÓNICA

Artículo 169.- Supervisión del Servicio de Vigilancia Electrónica. La Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, o quien haga sus veces, supervisará la correcta ejecución de los procedimientos administrativos, técnicos y operativos relacionados con el Servicio de Vigilancia Electrónica, conforme la normativa vigente, el presente Reglamento Técnico, instructivos, protocolos, formatos y demás instrumentos aplicables.

La supervisión podrá realizarse de manera permanente, periódica, aleatoria o específica, de acuerdo con la naturaleza del procedimiento, criticidad del caso, nivel de riesgo o necesidad institucional.

Artículo 170.- Finalidad de la supervisión. La supervisión tendrá como finalidad verificar el cumplimiento de las disposiciones judiciales, la correcta instalación, activación, monitoreo, soporte, desinstalación, registro, archivo, atención de alertas y alarmas, control de calidad, gestión de dispositivos dañados, pago, exoneración, reducción o diferimiento, así como la adecuada coordinación institucional e interinstitucional.

Artículo 171.- Responsables de la supervisión. La supervisión estará a cargo de los servidores designados por la unidad responsable, supervisores de monitoreo, responsables técnicos, responsables territoriales o demás servidores que, por sus funciones, intervengan en la gestión, control, seguimiento o evaluación del Servicio de Vigilancia Electrónica.

Los responsables de supervisión deberán actuar con objetividad, oportunidad, reserva, diligencia, trazabilidad y apego a la normativa aplicable.

Artículo 172.- Alcance de la supervisión. La supervisión del Servicio de Vigilancia Electrónica podrá comprender, entre otros aspectos:

a. Recepción y verificación de disposiciones judiciales;
b. Instalación, activación y parametrización de DVE;
c. Monitoreo y atención de eventos, alertas y alarmas;

d. Cumplimiento de tiempos de respuesta;
e. Escalamiento interno y externo;
f. Elaboración y remisión de informes;
g. Soporte técnico, sustitución, reposición y desinstalación;
h. Gestión de dispositivos dañados;
i. Registro, archivo y custodia de documentación;
j. Seguridad y reserva de la información;
k. Control de pagos, exoneraciones, reducciones y diferimientos;
l. Coordinación con autoridades competentes;
m. Cumplimiento de formatos, matrices, bitácoras y expedientes; y,
n. Implementación de acciones correctivas y de mejora continua.

Artículo 173.- Responsabilidad de los servidores intervinientes. Los servidores públicos y personal que intervengan en la gestión del Servicio de Vigilancia Electrónica serán responsables de cumplir las obligaciones, funciones, procedimientos, registros, plazos, protocolos, medidas de seguridad y lineamientos establecidos en el presente Reglamento Técnico y demás normativa aplicable.

Artículo 174.- Responsabilidad del personal técnico. El personal técnico será responsable de ejecutar correctamente los procedimientos de instalación, revisión, soporte, sustitución, reposición, desinstalación, diagnóstico, levantamiento de actas, informes, anexos fotográficos, georreferenciación y registro de actuaciones relacionadas con los Dispositivos de Vigilancia Electrónica.

Asimismo, deberá preservar la integridad del equipo, la seguridad del procedimiento técnico, la confidencialidad de la información y la trazabilidad documental de cada actuación.

Artículo 175.- Responsabilidad del personal de monitoreo. El personal de monitoreo será responsable de observar, validar, clasificar, atender, registrar, escalar, dar seguimiento y cerrar los eventos, alertas, alarmas y novedades generadas por el Sistema de Vigilancia Electrónica, conforme los niveles de criticidad, tiempos de respuesta, protocolos institucionales y disposiciones del presente Reglamento Técnico.

Artículo 176.- Responsabilidad de los supervisores. Los supervisores serán responsables de controlar la gestión del personal a su cargo, verificar la atención oportuna de eventos críticos, validar cierres cuando corresponda, revisar bitácoras, disponer escalamiento, solicitar informes, coordinar acciones internas o externas y reportar novedades relevantes a la autoridad institucional competente.

Artículo 177.- Responsabilidad de la unidad administrativa financiera. La unidad administrativa financiera competente será responsable, en el ámbito de sus atribuciones, de registrar, controlar, verificar y dar seguimiento a los valores recaudados por concepto de uso y mantenimiento del Dispositivo de Vigilancia Electrónica, así como de coordinar los aspectos relacionados con comprobantes, pagos, valores pendientes, registros financieros, control patrimonial y demás actuaciones administrativas que correspondan.

Artículo 178.- Responsabilidad de la unidad tecnológica. La unidad tecnológica competente, en coordinación con la unidad responsable del Servicio de Vigilancia Electrónica, brindará soporte en los aspectos relacionados con plataformas, sistemas, accesos, seguridad informática, interoperabilidad, respaldo de información, disponibilidad tecnológica, conectividad, usuarios institucionales, credenciales, incidentes tecnológicos y demás aspectos necesarios para el funcionamiento del Sistema de Vigilancia Electrónica.

Artículo 179.- Responsabilidad de los responsables territoriales. Los responsables territoriales o servidores designados en territorio deberán coordinar, ejecutar o apoyar, según corresponda, los procedimientos de instalación, soporte, sustitución, reposición, desinstalación, verificación de usuarios, levantamiento de información, remisión de expedientes, coordinación con autoridades locales y demás actuaciones necesarias para la gestión del Servicio de Vigilancia Electrónica.

Artículo 180.- Prohibiciones generales del personal interviniente. El personal que intervenga en la gestión

del Servicio de Vigilancia Electrónica tendrá prohibido:

a. Ejecutar actuaciones sin disposición judicial, respaldo documental o autorización institucional, cuando corresponda;
b. Omitir el registro de actuaciones, novedades, alertas, alarmas, soportes o comunicaciones;
c. Alterar, eliminar, ocultar o modificar información de la plataforma, expedientes, matrices o bitácoras;
d. Cerrar eventos sin validación, atención o justificación suficiente;
e. Divulgar información reservada, confidencial o de acceso restringido;
f. Usar credenciales institucionales de terceros o compartir las propias;
g. Manipular indebidamente dispositivos, registros, reportes o documentos;
h. Instalar, desinstalar, activar o desvincular dispositivos sin respaldo suficiente;
i. Utilizar equipos, imágenes, datos, registros o información institucional para fines ajenos al servicio;
j. Omitir la comunicación de incumplimientos, daños, cortes, alertas críticas o novedades relevantes; y,
k. Cualquier otra actuación contraria a la normativa vigente, al presente Reglamento Técnico o a los principios de seguridad, trazabilidad y responsabilidad.

Artículo 181.- Acciones correctivas. Cuando se identifiquen incumplimientos, debilidades, hallazgos, omisiones, errores, retrasos, fallas de registro o deficiencias operativas en la gestión del Servicio de Vigilancia Electrónica, la unidad responsable podrá disponer acciones correctivas, preventivas o de mejora.
Estas acciones podrán incluir actualización de procedimientos, ajustes de formatos, fortalecimiento de controles, redistribución de funciones, seguimiento específico de casos, auditorías internas, mejoras tecnológicas o cualquier otra medida necesaria. Las acciones de capacitación, inducción y retroalimentación del personal se sujetarán a la norma específica prevista en el artículo 182 del presente Reglamento Técnico.

Artículo 182.- Capacitación del personal. La unidad responsable promoverá procesos de capacitación, inducción, actualización y retroalimentación dirigidos al personal que intervenga en la gestión del Servicio de Vigilancia Electrónica, especialmente en materia de instalación, monitoreo, atención de alertas, soporte técnico, seguridad de la información, reserva documental, uso de plataforma, gestión de dispositivos dañados, pagos y responsabilidades.

Artículo 183.- Evaluación del desempeño operativo. La unidad responsable podrá implementar mecanismos de evaluación del desempeño operativo del personal que intervenga en el Servicio de Vigilancia Electrónica, considerando indicadores de cumplimiento, oportunidad, trazabilidad, calidad de registros, atención de eventos, gestión de alertas, control documental y aplicación de procedimientos.

Artículo 184.- Indicadores de gestión. Para medir la eficiencia, oportunidad y calidad del Servicio de Vigilancia Electrónica, la unidad responsable podrá establecer indicadores de gestión, tales como:

a. Número de disposiciones judiciales recibidas;
b. Número de DVE instalados;
c. Tiempo promedio de instalación;
d. Número de instalaciones no ejecutadas y sus causas;
e. Número de usuarios monitoreados;
f. Número de alertas y alarmas generadas;
g. Porcentaje de alertas atendidas dentro del tiempo establecido;
h. Número de eventos críticos escalados;
i. Número de informes remitidos a autoridad competente;
j. Número de dispositivos dañados, sustituidos o no recuperados;
k. Número de desinstalaciones ejecutadas;
l. Número de solicitudes de exoneración, reducción o diferimiento;
m. Valores recaudados, pendientes o diferidos, cuando corresponda; y,
n. Otros indicadores que permitan evaluar la gestión institucional.

Artículo 185.- Mejora continua. La gestión del Servicio de Vigilancia Electrónica deberá orientarse a la

mejora continua de sus procedimientos, formatos, matrices, sistemas, tiempos de respuesta, mecanismos de supervisión, criterios de clasificación, canales de coordinación y medidas de seguridad de la información.

Las mejoras podrán derivarse de hallazgos, informes de calidad, auditorías, evaluación de indicadores, cambios normativos, necesidades operativas, incorporación de nueva tecnología o disposiciones de autoridad competente.

Artículo 186.- Actualización de instrumentos técnicos. Los instructivos, protocolos, formatos, matrices, flujogramas, anexos y demás instrumentos técnicos derivados del presente Reglamento Técnico podrán ser actualizados por la unidad responsable, conforme las necesidades institucionales, cambios normativos, mejoras operativas o implementación de nuevas herramientas tecnológicas.
Las actualizaciones deberán ser socializadas al personal correspondiente y registradas en los documentos de control institucional.

Artículo 187.- Reporte de riesgos operativos. Los servidores que identifiquen riesgos operativos, tecnológicos, documentales, patrimoniales, financieros, jurídicos o de seguridad relacionados con el Servicio de Vigilancia Electrónica deberán reportarlos de manera oportuna al responsable inmediato superior o a la unidad competente.

El reporte de riesgos deberá permitir la adopción de medidas preventivas, correctivas o de contingencia.

DISPOSICIONES GENERALES

PRIMERA. - Aplicación obligatoria. Las disposiciones contenidas en la presente Resolución, así como los instructivos, protocolos, formatos, matrices y demás instrumentos técnicos derivados de esta, serán de aplicación obligatoria para todas las unidades administrativas, servidores públicos, personal técnico, operadores de monitoreo, supervisores, responsables territoriales y demás personal que intervenga directa o indirectamente en la gestión del Servicio de Vigilancia Electrónica.

SEGUNDA. - Instrumentos complementarios. La Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, o quien haga sus veces, podrá elaborar, actualizar y proponer instructivos, protocolos, formatos, matrices, guías, flujogramas, anexos técnicos y demás instrumentos complementarios necesarios para la adecuada implementación del Reglamento Técnico.

TERCERA. - Coordinación interna. Las unidades administrativas, financieras, jurídicas, tecnológicas, territoriales, de planificación, seguridad penitenciaria y demás áreas del SNAI deberán coordinar, en el ámbito de sus competencias, las acciones necesarias para la implementación, ejecución, control, seguimiento y mejora continua del Servicio de Vigilancia Electrónica.

CUARTA. - Confidencialidad. La información, documentación, expedientes, registros, matrices, reportes, anexos fotográficos, geocercas, alertas, alarmas, novedades, datos personales, parámetros técnicos y demás información generada o administrada dentro del Servicio de Vigilancia Electrónica tendrá carácter reservado, confidencial o de acceso restringido, según corresponda.

Su acceso, uso, reproducción, remisión o entrega deberá sujetarse a la normativa vigente, a los canales oficiales y a criterios de competencia, necesidad institucional, seguridad de la información y protección de datos personales.

QUINTA. - Responsabilidad por incumplimiento. La inobservancia de las disposiciones contenidas en la presente Resolución, así como en los instructivos, protocolos, formatos, matrices o demás instrumentos institucionales derivados de esta, podrá generar responsabilidades administrativas, civiles o penales, conforme la normativa vigente.

SEXTA. - Interpretación y absolución de consultas. Las dudas relacionadas con la aplicación del Reglamento Técnico serán conocidas y absueltas por la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, en coordinación con la unidad jurídica institucional, cuando corresponda.

SÉPTIMA. - Actualización normativa. En caso de reforma, sustitución o expedición de nueva normativa relacionada con el Servicio de Vigilancia Electrónica, medidas no privativas de libertad, regímenes penitenciarios, dispositivos electrónicos, pagos, exoneraciones, protección de datos, seguridad de la información o gestión documental, la unidad responsable deberá revisar y proponer las actualizaciones necesarias al Reglamento Técnico.

OCTAVA. - Ejecución. Encárguese la ejecución de la presente Resolución a la Subdirección de Medidas Cautelares, Ejecución de Penas y Medidas Socioeducativas; a la Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción; y a las demás unidades administrativas del SNAI, dentro del ámbito de sus competencias.

NOVENA. - Publicación y socialización. Dispóngase la publicación y socialización de la presente Resolución a través de los canales institucionales correspondientes, para conocimiento y aplicación obligatoria de los servidores públicos y personal relacionado con la gestión del Servicio de Vigilancia Electrónica.

DECIMA. - Notificación. Encárguese a la Dirección Administrativa o a la unidad que corresponda la notificación de la presente Resolución a las unidades administrativas involucradas, para su conocimiento, cumplimiento y aplicación.

DISPOSICIONES TRANSITORIAS

PRIMERA. - Implementación progresiva. La implementación del Reglamento Técnico se realizará de manera progresiva, de acuerdo con la disponibilidad técnica, operativa, administrativa, financiera, tecnológica y territorial del SNAI, sin perjuicio de la aplicación inmediata de las disposiciones relacionadas con seguridad de la información, reserva documental, registro de actuaciones y atención de alertas o alarmas críticas.

SEGUNDA. - Actualización de formatos y matrices. La Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, en coordinación con las unidades competentes, revisará y actualizará los formatos, matrices, actas, informes, bitácoras y demás instrumentos de registro necesarios para la aplicación del Reglamento Técnico.

TERCERA. - Socialización del Reglamento Técnico. La unidad responsable coordinará la socialización del Reglamento Técnico con el personal técnico, operadores de monitoreo, supervisores, responsables territoriales y demás servidores vinculados con la gestión del Servicio de Vigilancia Electrónica.

CUARTA. - Capacitación inicial. La unidad responsable podrá coordinar procesos de capacitación, inducción o retroalimentación dirigidos al personal que intervenga en la gestión del Servicio de Vigilancia Electrónica, con la finalidad de fortalecer la aplicación uniforme de los procedimientos establecidos en el Reglamento Técnico.

QUINTA. - Regularización documental. Los expedientes, matrices, registros o documentos generados con anterioridad a la expedición de la presente Resolución podrán ser regularizados, actualizados o incorporados progresivamente a los repositorios institucionales correspondientes, conforme la disponibilidad documental, operativa y tecnológica.

SEXTA. - Adecuación de sistemas y plataformas. Las unidades competentes coordinarán, según corresponda, la adecuación, actualización o fortalecimiento de los sistemas, plataformas, repositorios y herramientas tecnológicas necesarias para la implementación del Reglamento Técnico.

Resolución Nro. SNAI-SNAI-2026-0052-R

Quito, D.M., 15 de mayo de 2026

SÉPTIMA. - Procedimientos en trámite. Los procedimientos de instalación, monitoreo, soporte técnico, desinstalación, gestión de dispositivos dañados, control de calidad, pago, exoneración, reducción o diferimiento que se encuentren en trámite a la fecha de expedición de la presente Resolución continuarán sustanciándose conforme el estado en que se encuentren, procurando su adecuación progresiva a las disposiciones del Reglamento Técnico.

OCTAVA. - Cambio progresivo de dispositivos previamente instalados. La Dirección de Penas No Privativas de Libertad, Dispositivos de Vigilancia Electrónica y Reinserción, o quien haga sus veces, coordinará y ejecutará, en el plazo máximo de noventa (90) días contados a partir de la suscripción de la presente Resolución, el cambio progresivo de los Dispositivos de Vigilancia Electrónica que se encuentren instalados con anterioridad a su expedición, cuando por razones técnicas, operativas, tecnológicas, contractuales, de seguridad, renovación del sistema, compatibilidad con la plataforma institucional, disponibilidad de equipos, falla permanente, estado del dispositivo o necesidad del servicio resulte procedente su sustitución o reemplazo.
Para el efecto, la unidad responsable deberá priorizar los casos conforme criterios de criticidad, continuidad del monitoreo, estado del dispositivo, nivel de riesgo, modalidad de vigilancia, alertas recurrentes, fallas técnicas, ubicación territorial y disponibilidad operativa, procurando que el cambio se ejecute de manera ordenada, planificada y sin afectar la prestación del Servicio de Vigilancia Electrónica.

El cambio de los dispositivos previamente instalados deberá documentarse mediante acta, informe, registro de plataforma, actualización del número de serie, anexo fotográfico y demás respaldos que correspondan, garantizando la continuidad del monitoreo y la trazabilidad del procedimiento.
La ejecución del cambio de dispositivo no alterará las condiciones judiciales impuestas a la persona monitoreada ni suspenderá la obligación institucional de mantener el seguimiento mientras se encuentre vigente la disposición emitida por autoridad competente. Cuando corresponda, se notificará a la autoridad jurisdiccional competente.

DISPOSICIÓN DEROGATORIA

ÚNICA. - Derogatoria. Deróguense todas las disposiciones, instrumentos, lineamientos, directrices, procedimientos, formatos o actos administrativos de igual o menor jerarquía que se opongan a lo dispuesto en la presente Resolución.

DISPOSICIONES FINALES

ÚNICA. - La presente resolución entrará en vigor a partir de la fecha de su suscripción, sin perjuicio de su socialización institucional y de su publicación en el Registro Oficial.

Dado y suscrito en la ciudad de Quito, Distrito Metropolitano, a los catorce días del mes de mayo del año 2026.

Con sentimientos de distinguida consideración.

Documento firmado electrónicamente

Mgs. Mauricio Fernando Mayorga Vallejo
DIRECTOR GENERAL

REPÚBLICA DEL ECUADOR

Resolución Nro. SNAI-SNAI-2026-0052-R

Quito, D.M., 15 de mayo de 2026

il/aj/es/ac/ha

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MAURICIO FERNANDO MAYORGA VALLEJO