GASPOCH
GASOLINERA POLITÉCNICA E.P

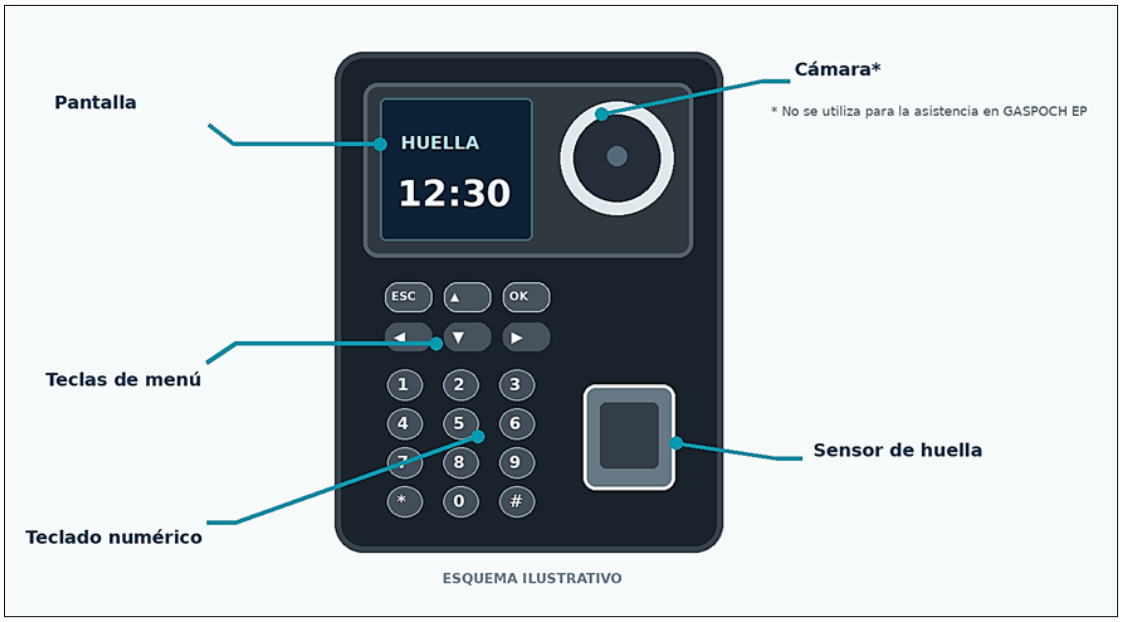
MANUAL INTEGRAL DE USO Y OPERACIÓN DEL SISTEMA BIOMÉTRICO

HIKVISION DS-K1T320MFX

Registro de asistencia del personal mediante huella dactilar

Estación de Servicios ESPOCH Gasolinera Politécnica E.P.

Riobamba · Noviembre de 2026



Enfoque del manual

Este documento reúne los antecedentes institucionales, los hallazgos de la evaluación de impacto, la justificación técnica, el marco de protección de datos y los procedimientos de operación del equipo. Describe el uso institucional reportado, sin sustituir la determinación jurídica que exige la normativa para tratar huellas dactilares.

Panamericana Sur Km 1 ½ y 11 de Noviembre.

+593 (03) 2 318-163

www.gasolineraespochep.ec

1. ANTECEDENTES

La Estación de Servicios ESPOCH Gasolinera Politécnica E.P., utiliza un sistema biométrico para el registro y control de asistencia de su personal, con la finalidad de registrar y verificar el cumplimiento de las jornadas laborales, así como disponer de información que permita realizar el seguimiento correspondiente por parte de las áreas administrativas competentes.

El presente manual describe el funcionamiento y uso del sistema biométrico de GASPOCH EP, tomando como referencia la evaluación de impacto en protección de datos personales, el informe técnico justificativo del uso de huella dactilar y la normativa aplicable. Además, establece las instrucciones para el manejo del terminal Hikvision DS-K1T320MFX y del software iVMS-4200, dirigidas al personal de la institución de acuerdo a sus respectivas funciones.

1.1. Evaluación de impacto en protección de datos personales

La evaluación de impacto en protección de datos personales del sistema biométrico de la Estación de Servicios ESPOCH Gasolinera Politécnica E.P., identifica como información involucrada los datos de identificación, las huellas dactilares y los registros de asistencia, utilizados para registrar y controlar la asistencia del personal.

La evaluación aplica una valoración cualitativa basada en probabilidad e impacto, y distingue el riesgo residual que subsiste después de considerar los controles existentes.

Riesgo identificado	Nivel de riesgo	Medidas de seguridad y riesgos residuales
Acceso no autorizado a datos biométricos	Probabilidad baja · Impacto alto	Constan contraseña administrativa y restricción de acceso mediante red institucional. Continúa el riesgo de credenciales comprometidas.
Uso o conservación inadecuados de huellas	Probabilidad media · Impacto alto	La evaluación registra eliminación de huellas del personal desvinculado por Talento Humano; persiste riesgo por procedimientos de conservación insuficientemente documentados.
Pérdida de registros por fallas técnicas	Probabilidad media · Impacto medio	Se descargan reportes de asistencia, pero la evaluación no acredita respaldos integrales del sistema; persiste riesgo de pérdida de información.

La evaluación concluye que los controles de acceso y seguridad contribuyen a reducir la exposición, pero no eliminan los riesgos. También señala la necesidad de justificar jurídicamente el tratamiento de huellas, fortalecer la conservación y eliminación, y establecer mecanismos de respaldo y recuperación.

Medidas de seguridad y control del sistema biométrico

Los resultados de la evaluación de impacto permiten identificar los riesgos asociados al tratamiento de datos biométricos y las medidas necesarias para garantizar la seguridad de la información. A continuación, se presentan los principales aspectos identificados en dicha evaluación, junto con las medidas de seguridad y control existentes y las acciones de mejora propuestas para el sistema biométrico de GASPOCH E.P.

Aspectos identificados en la evaluación de impacto	Medidas de seguridad y control del sistema
Dato biométrico sensible; impacto alto si existe acceso indebido	El dispositivo se utiliza institucionalmente solo con huella; el acceso administrativo se limita a personal con funciones asignadas y a la red interna.
Riesgo por uso y conservación de plantillas	El enrolamiento y las bajas se gestionan de forma controlada, con tratamiento mínimo y sin compartir huellas o datos de usuarios por canales personales.
Riesgo de pérdida de registros; respaldos integrales no acreditados	Se consulta y exporta asistencia en iVMS-4200; la evaluación incluye como acción de mejora establecer respaldo y recuperación verificables.
Necesidad de trazabilidad e integridad	Las marcaciones originales permanecen sin corrección ni sustitución; las novedades administrativas se documentan aparte.
Necesidad de controles y seguimiento continuo	TICS verifica los accesos y el funcionamiento del equipo; incidentes y anomalías se comunican según las competencias institucionales.

1.2. Informe técnico justificativo del uso de huella dactilar

El Informe Técnico Nro.- 003-GASPOCH-EP-2026-TICS, de 7 de noviembre de 2026, expone la conveniencia operativa de la huella para vincular cada marcación a una característica individual y reducir el uso de credenciales intercambiables. El informe compara los mecanismos posibles en las condiciones presupuestarias y operativas descritas por TICS:

Mecanismo	Ventaja o limitación identificada
Tarjeta de proximidad	Permite marcar rápidamente, pero puede prestarse o perderse. El informe indica que su adquisición no estaba contemplada en el presupuesto vigente.
Código PIN	Evita el tratamiento de huellas, pero el código puede compartirse y requiere medidas adicionales de verificación.
Registro manual	No requiere biometría, aunque demanda mayor intervención administrativa y controles de confiabilidad.

Mecanismo	Ventaja o limitación identificada
Huella dactilar	Vincula la marcación al trabajador sin tarjeta ni código transferible, aprovechando el equipo existente; implica tratar un dato sensible.

El informe determina que, desde el punto de vista técnico y de los recursos disponibles, la huella es la alternativa más conveniente de las analizadas. Esta conclusión es técnica: debe leerse junto con la evaluación de impacto y la exigencia jurídica.

2. MARCO NORMATIVO APLICABLE

El marco jurídico se refiere tanto a la obligación institucional de controlar la asistencia como a las garantías que deben observarse cuando ese control involucra datos personales sensibles:

Norma o instrumento	Relación con el manual
Constitución de la República del Ecuador, art. 66 numeral 19	Reconoce el derecho a la protección de datos personales y exige respeto a su tratamiento y circulación.
Ley Orgánica de Protección de Datos Personales (LOPDP)	Define datos personales y biométricos, principios de tratamiento, información a los titulares, bases de legitimación, datos sensibles, seguridad y evaluación de impacto (especialmente arts. 4, 7, 10, 12, 25, 26 y 42).
Reglamento General a la LOPDP, Decreto Ejecutivo 904	Desarrolla la evaluación de impacto, su obligatoriedad y contenido (arts. 29, 31 y 32).
Resolución SPDP-SPD-2026-0039-R: Norma General para el Tratamiento de Datos Biométricos	Exige analizar riesgos y necesidad, establecer base jurídica válida, proteger datos desde el diseño, incorporar seguridad reforzada y revisar periódicamente la EIPD (arts. 5, 6, 13, 14, 15 y 16).
Guía SPDP de gestión de riesgos y evaluación de impacto, versión 2 (2026)	Aporta criterios metodológicos para identificar, valorar y tratar riesgos a los derechos de los titulares.
Reglamento de Administración del Talento Humano de GASPOCH EP, arts. 55 y 56	Según el Manual y Política institucional, establece control de jornada y asistencia y atribuye competencias a la Unidad de Administración del Talento Humano.
Manual y Política para la Gestión del Sistema Biométrico de GASPOCH EP	Es el instrumento institucional de referencia para funciones, accesos, información al titular, integridad de marcaciones, conservación, incidentes y mecanismos alternativos.

2.1. Alcance jurídico de la justificación técnica

El registro de asistencia es una finalidad administrativa identificada. Sin embargo, la necesidad de registrar asistencia no demuestra automáticamente que sea indispensable emplear huellas dactilares. Por tratarse de un dato sensible, la institución debe sustentar la base de legitimación aplicable, la necesidad y proporcionalidad de este mecanismo y

la valoración de alternativas menos invasivas, en los términos de la LOPDP y la normativa de la SPDP.

El Manual y Política institucional examina como referencia el supuesto laboral del artículo 26 literal b) de la LOPDP, pero lo presenta como causal a sustentar, no como habilitación automáticamente acreditada. El presente documento describe la tecnología y los controles operativos; no sustituye ese análisis jurídico.

2.2. Consecuencias para la operación cotidiana

- **Finalidad limitada.** La información se utiliza para asistencia y gestión administrativa asociada; no debe convertirse en un sistema de vigilancia personal con otros fines.
- **Información y derechos.** Antes de captar una huella, se siguen las disposiciones institucionales sobre aviso de privacidad, derechos y mecanismo no biométrico.
- **Acceso proporcional.** Cada función utiliza solo los datos indispensables; se restringe el acceso a plantillas, usuarios y reportes.
- **Seguridad reforzada.** Se exige control administrativo, integridad de eventos, medidas de protección en exportaciones y gestión de incidencias.

3. IDENTIFICACIÓN Y FUNCIONAMIENTO TÉCNICO DEL EQUIPO

Componente	Configuración o uso institucional
Terminal	Hikvision DS-K1T320MFX, serie DS-K1T320.
Lectura para asistencia	Sensor de huella dactilar. No se utiliza reconocimiento facial para las marcaciones.
Interfaz	Pantalla, teclas de menú/confirmación y lector de huella del equipo.
Conectividad	Comunicación por dirección IP dentro de la red institucional.
Plataforma de consulta	Software Hikvision iVMS-4200 instalado en la computadora de TICS.
Marcaciones	Ingreso: opción 1. Salida: opción 2
Funciones adicionales del fabricante	Rostro, tarjeta, PIN y control de acceso físico; su disponibilidad técnica no implica utilización institucional.

El dispositivo identifica la huella registrada, genera un evento de asistencia asociado a un identificador y a su fecha y hora y permite consultar los registros mediante el entorno administrativo institucional. El modo exacto de comparación biométrica y otros parámetros internos pertenecen a la configuración técnica controlada por TICS.

3.1. Componentes visibles del terminal



Figura 1. Identificación de los componentes principales del terminal biométrico Hikvision DS-K1T320MFX.

- **Pantalla.** Muestra hora, menús y mensajes de autenticación.
- **Sensor de huella.** Captura la muestra necesaria para cotejar con la plantilla registrada.
- **Teclas de menú.** Permiten seleccionar opciones y gestionar menús autorizados.
- **Teclado numérico.** Forma parte del hardware; su presencia no implica que se utilice PIN en el registro de asistencia.
- **Cámara integrada.** Existe en el equipo, pero no se usa institucionalmente para reconocimiento facial en asistencia.

3.2. Proceso de registro de asistencia mediante huella dactilar

El sistema biométrico permite registrar la asistencia del personal mediante la autenticación de huellas dactilares previamente registradas en el terminal Hikvision DS-K1T320MFX. El proceso comprende las siguientes etapas:

1. **Autenticación biométrica:** El trabajador coloca su dedo sobre el sensor de huella dactilar para que el dispositivo realice la verificación correspondiente.
2. **Selección del tipo de marcación:** El trabajador selecciona la opción correspondiente al registro de entrada o salida, de acuerdo con la configuración institucional.
3. **Validación de identidad:** El terminal compara la información biométrica capturada con las plantillas registradas y determina si la autenticación es válida.
4. **Registro de asistencia:** Cuando la autenticación es satisfactoria, el sistema registra la marcación con la identificación del trabajador, la fecha y la hora correspondientes.
5. **Consulta de información:** Los registros de asistencia pueden consultarse mediante el software iVMS-4200, desde el cual el área de TICS realiza la búsqueda y generación de reportes según los requerimientos institucionales.

3.3. Procedimiento de marcación para el personal

Para registrar correctamente la asistencia mediante el terminal biométrico, los trabajadores deberán seguir el procedimiento que se detalla a continuación:

Paso 1. Verificar el estado del dispositivo
Comprobar que el terminal biométrico se encuentre encendido y que su pantalla esté funcionando correctamente.

Paso 2. Registrar la huella dactilar.
Colocar el dedo previamente registrado sobre el sensor de huella dactilar, procurando que esté limpio y seco. Mantenerlo en la superficie de lectura hasta que el dispositivo complete el proceso de autenticación.

Paso 3. Seleccionar el tipo de marcación
Elegir la opción correspondiente al movimiento que se desea registrar, conforme a la configuración establecida en GASPOCH E.P.:

- **Entrada (1):** Registro de ingreso a la jornada laboral.
- **Salida (2):** Registro de salida de la jornada laboral.

Paso 4. Verificar la confirmación de la marcación.
Comprobar que el terminal muestre el mensaje o señal de autenticación satisfactoria. Si el dispositivo presenta un error, repetir el procedimiento sin realizar intentos excesivos.

Paso 5. Comunicar inconvenientes en el registro.
Si el dispositivo no reconoce la huella dactilar o presenta fallas que impidan registrar la asistencia, el trabajador deberá comunicar la novedad al área de Talento Humano para que se gestione conforme a los procedimientos institucionales.

Integridad de los registros de asistencia

Los registros originales de entrada y salida generados por el sistema biométrico deberán conservarse sin modificaciones, correcciones ni sustituciones. Las novedades relacionadas con atrasos, ausencias, omisiones de marcación u otras situaciones administrativas serán gestionadas por el área de Talento Humano mediante los procedimientos correspondientes, sin alterar la información registrada originalmente en el dispositivo.

4. Gestión de usuarios y huellas

4.1. Enrolamiento de personal autorizado

La documentación operativa de GASPOCH E.P., identifica a Talento Humano como el área que realiza en el terminal el registro de usuarios y huellas. La operación debe ajustarse a la información y modalidad de asistencia que corresponda a cada trabajador.

4.2. Baja y eliminación de huellas

Cuando concluye la relación laboral, se adopta un mecanismo alternativo o deja de existir la finalidad de tratamiento, se activa la gestión de baja. En la práctica descrita por la evaluación de impacto, Talento Humano elimina los registros de huella en el terminal. Las responsabilidades formales, plazos, tratamiento de copias y constancia de supresión se rigen por el apartado 13 del “Manual y Política para la Gestión del Sistema Biométrico”, que prevalece sobre esta explicación práctica.

Paso 1. Identificar correctamente
Localizar el usuario por su identificador institucional y confirmar que se trata del registro correspondiente.

Paso 2. Operar solo sobre el titular
Utilizar las funciones individuales de eliminación autorizadas; no ejecutar borrados globales de usuarios o del dispositivo.

Paso 3. Documentar la actuación
Registrar la novedad conforme a los formatos y responsabilidades institucionales, incluida la intervención técnica de TICS cuando corresponda.

Paso 4. Separar los datos históricos
La supresión de una plantilla biométrica no equivale a borrar automáticamente los eventos de asistencia conservados por razones administrativas o legales.

5. Consulta y generación de reportes en iVMS-4200

El sistema biométrico Hikvision DS-K1T320MFX se encuentra conectado a la red institucional de GASPOCH E.P., lo que permite la consulta de los registros de asistencia mediante el software iVMS-4200. Esta aplicación facilita la visualización de las marcaciones de entrada y salida del personal, así como la generación de reportes correspondientes a períodos determinados. La administración técnica del sistema y la generación de reportes están a cargo de TICS, mientras que Talento Humano utiliza la información para el control y seguimiento de la asistencia laboral, de acuerdo con sus competencias. El acceso y tratamiento de estos registros se limita al personal autorizado, garantizando la confidencialidad, integridad y uso adecuado de los datos personales, conforme a las medidas de seguridad institucionales y la normativa vigente en materia de protección de datos personales.

6. Responsabilidad en el uso institucional

Actor	Responsabilidad en el sistema
Trabajadores	Realizar personalmente entrada y salida, cuidar el sensor y reportar problemas de lectura o marcación.
Talento Humano	Administrar el control de asistencia, registrar huellas y gestionar novedades y desvinculaciones según práctica documentada y reglas institucionales.
TICS	Administrar técnicamente el equipo, conectividad e iVMS-4200, revisar seguridad y generar reportes institucionales autorizados.
Delegado de Protección de Datos	Brindar asesoría especializada en protección de datos, riesgos, información a titulares, derechos e incidentes conforme a sus atribuciones.

7. Seguridad, confidencialidad y protección de datos

- **Control de acceso.** Emplear cuentas individuales, restringir el menú administrativo y no divulgar credenciales o configuración sensible.
- **Red institucional.** Mantener la administración dentro del entorno institucional; no habilitar servicios en nube ni accesos externos sin el procedimiento correspondiente.
- **Datos mínimos.** Registrar únicamente identificadores y datos imprescindibles; el uso de cámara, rostro o control de puertas no forma parte de la finalidad descrita.

- **Separación de funciones.** Distinguir la administración de huellas y personal, la gestión técnica y la evaluación administrativa de los reportes.
- **Exportaciones.** No remitir listados por correos personales, mensajería no institucional ni memorias USB particulares.
- **Conservación y eliminación.** Atender el régimen institucional para plantillas biométricas y registros de asistencia, que son categorías distintas.
- **Incidentes y derechos.** Comunicar posibles accesos indebidos, pérdida de información o solicitudes de titulares a las áreas competentes, evitando accesos o comunicaciones no autorizadas.

8. Mantenimiento preventivo y medidas de cuidado

- **Sensor.** Limpiar suavemente con paño seco que no desprenda pelusa. No aplicar alcohol o líquidos directamente sobre el lector ni usar elementos abrasivos.
- **Pantalla y carcasa.** Evitar golpes, humedad excesiva, cambios de ubicación y manipulación de la cubierta del dispositivo.
- **Alimentación y red.** No desconectar, sustituir adaptadores, intervenir cableado o reiniciar el terminal sin actuación técnica autorizada.
- **Hora y fecha.** TICS verifica la configuración horaria porque la integridad de las marcaciones depende de registros temporales confiables.
- **Software y firmware.** Las actualizaciones y cambios de configuración deben ser planificados por TICS, contemplando continuidad, seguridad y conservación de evidencia.
- **Pruebas técnicas.** Verificar disponibilidad, acceso de usuarios autorizados, comunicación con iVMS-4200 y correcta consulta de eventos sin modificar históricos.

9. Disposiciones generales para el uso del sistema biométrico

El sistema biométrico de GASPOCH E.P., deberá utilizarse exclusivamente para el registro y control de asistencia del personal, de acuerdo con los procedimientos institucionales y las disposiciones aplicables en materia de protección de datos personales.

La administración y utilización del sistema estarán sujetas a las responsabilidades asignadas a las áreas de Talento Humano y TICS, garantizando el acceso restringido a la información, la confidencialidad de los datos personales y la integridad de los registros de asistencia.

Las actividades relacionadas con el uso, mantenimiento y administración del dispositivo deberán realizarse conforme a las medidas de seguridad institucionales, procurando su correcto funcionamiento y la protección de la información registrada.