



UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

VICERRECTORADO ACADÉMICO GENERAL

**POLÍTICA ESPECÍFICA DE PROTECCIÓN DE DATOS PERSONALES DE LA
UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE**

COD: USIN-PLE-2025-V2-038

JULIO- 2025

 <p>ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACIÓN PARA LA EXCELENCIA</p>	<p>POLÍTICA ESPECÍFICA DE PROTECCIÓN DE DATOS PERSONALES DE LA UNIVERSIDAD DE FUERZAS ARMADAS - ESPE</p>	<p>Vicerrectorado Académico General Vicerrectorado Administrativo Unidad de Asesoría Jurídica Unidad de Seguridad Integrada</p> <hr/> <p>Página: 2 de 19</p>
--	---	--

CONTENIDO

A. OBJETO..... 3

B. REFERENCIAS LEGALES..... 3

C. DEFINICIONES..... 6

D. PRINCIPIOS..... 8

E. DECLARACIÓN ESTATUTARIA..... 9

F. ÁMBITO DE APLICACIÓN..... 9

G. LINEAMIENTOS GENERALES PARA EL TRATAMIENTO DE DATOS PERSONALES..... 9

Obligaciones y Responsabilidades de la Universidad como Responsable del Tratamiento de Datos Personales. 9

Valoración de Riesgos en el Tratamiento de Datos Personales..... 11

Legitimidad del Tratamiento de Datos Personales..... 11

Plazo de Conservación de Datos Personales..... 12

Confidencialidad de la Información..... 12

Finalidades del Tratamiento de Datos Personales..... 13

Destinatarios a Terceros de Datos Personales..... 13

Registro y uso de cookies en sitios web..... 13

Derechos de los Titulares..... 14

Medidas para precautelar la seguridad de los datos personales..... 15

H. ROLES DE LA PROTECCIÓN DE DATOS PERSONALES..... 15

I. RESPONSABILIDAD EN EL MANEJO DE DATOS PERSONALES..... 17

J. ANEXO..... 17

K. CONTROL DE CAMBIOS..... 17

L. APROBACIÓN..... 18

A. OBJETO

El objeto de la Política de Protección de Datos Personales de la Universidad de las Fuerzas Armadas (ESPE) es garantizar el cumplimiento de los derechos fundamentales de los titulares de los datos personales, conforme a la normativa vigente. Esta política establece los principios, directrices y procedimientos para el tratamiento adecuado de los datos personales, asegurando su confidencialidad, integridad y disponibilidad. Además, busca proporcionar un marco de seguridad para proteger la información de los miembros de la comunidad universitaria, frente a riesgos, accesos no autorizados, alteraciones o pérdidas. La política también promueve la transparencia, el respeto a la privacidad y el ejercicio de los derechos de los titulares de los datos, contribuyendo a una cultura de protección de la información dentro de la institución.

B. REFERENCIAS LEGALES

1.1. Declaración Universal de Derechos Humanos:

Artículo 12: *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques"*.

1.2. Constitución de la República del Ecuador:

Numeral 19 del artículo 66: *"(...)El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley (...)"*;

Artículo 82: *"El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes"*;

Artículo 92: *"(...) Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados (...)"*;

Artículo 226: *"(...)Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. 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 (...)"*;

1.3. Código Orgánico Administrativo

Artículo 3: *“Principio de eficacia. Las actuaciones administrativas se realizan en función del cumplimiento de los fines previstos para cada órgano o entidad pública, en el ámbito de sus competencias.”;*

Artículo 4: *“Principio de eficiencia. Las actuaciones administrativas aplicarán las medidas que faciliten el ejercicio de los derechos de las personas. Se prohíben las dilaciones o retardos injustificados y la exigencia de requisitos puramente formales.”;*

Artículo 15: *“Principio de responsabilidad. El Estado responderá por los daños como consecuencia de la falta o deficiencia en la prestación de los servicios públicos o las acciones u omisiones de sus servidores públicos o los sujetos de derecho privado que actúan en ejercicio de una potestad pública por delegación del Estado y sus dependientes, controlados o contratistas.”;*

Artículo 21: *“Principio de ética y probidad. Los servidores públicos, así como las personas que se relacionan con las administraciones públicas, actuarán con rectitud, lealtad y honestidad. En las administraciones públicas se promoverá la misión de servicio, probidad, honradez, integridad, imparcialidad buena fe, confianza mutua, solidaridad, transparencia, dedicación al trabajo, en el marco de los más altos estándares profesionales; el respeto a las personas, la diligencia y la primacía del interés general, sobre el particular.”;*

Artículo 22: *“Principios de seguridad jurídica y confianza legítima. Las administraciones públicas actuarán bajo los criterios de certeza y previsibilidad (...).”.*

1.4. Código Orgánico Integral Penal:

Artículo 178: *“(...) Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley (...).”.*

Artículo 179: *“Revelación de secreto.- La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año.”.*

Artículo. 229: *“(...) Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.*

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años (...).”.

1.5. Ley Orgánica del Sistema Nacional de Registro de Datos Públicos:

Artículo 4: *"Responsabilidad de la información. - Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información (...)"*;

Artículo 6: *"Accesibilidad y confidencialidad.- Son confidenciales los datos de carácter personal. El acceso a estos datos, sólo será posible cuando quien los requiera se encuentre debidamente legitimado, conforme a los parámetros previstos en la Ley Orgánica de Protección de Datos Personales, su respectivo reglamento y demás normativa emitida por la Autoridad de Protección de Datos Personales (...)"*.

1.6. Ley Orgánica de Telecomunicaciones:

Artículo 78.- Seguridad de los Datos Personales: *"(Sustituido por el lit. a del num. 2 de la Disp. Reformatoria Cuarta de la Ley s/n, R.O. 459-5S, 26-V-2021).- Las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas, organizativas y de cualquier otra índole adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos personales de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales"*.

1.7. Ley Orgánica de Protección de Datos Personales:

Numeral 4 del artículo 47 de la Ley Orgánica de Protección de Datos Personales, expresa: *"El responsable del tratamiento de datos personales está obligado a: (...) 4) Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular (...)"*;

Numeral 3 del artículo 67 de la norma ibídem, establece: *"Se consideran infracciones leves las siguientes: (...) "No mantener disponibles políticas de protección de datos personales afines al tratamiento de datos personales (...)"*;

Literal f del artículo 26, establece *"el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos (...)"*.

1.8. Reglamento a la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos:

Art. 5: *"Responsables de las bases de datos.- El responsable de la información correspondiente a los entes registrales es la máxima autoridad de cada una de las instituciones. Los entes del Sistema deberán comunicar a la Dirección Nacional de Registro de Datos Públicos el nombre del funcionario que gestione la base de datos. En ningún caso el ente registral podrá estar sin un delegado institucional, que será el responsable de la administración de las bases de datos públicos y su correcto funcionamiento (...)"*.

1.9. Reglamento a la Ley Orgánica de Protección de Datos Personales:

Art. 1.- Objeto.- El presente Reglamento General tiene por objeto desarrollar la normativa para la aplicación de la Ley Orgánica de Protección de Datos Personales y la protección de los derechos y libertades fundamentales de los titulares de datos personales.

1.10. Orden de Rectorado Nro. 2025-042-ESPE-a-1

El señor Rector de la Universidad de las Fuerzas Armadas – ESPE, resuelve: “Art. 1.- *Aprobar y poner en vigencia, las Políticas Generales de Gestión Institucional marzo 2025, de la Universidad de las Fuerzas Armadas – ESPE, en los términos que expresamente se detalla en el documento que en nueve (09) fojas útiles, se anexa a la presente Orden de Rectorado, como parte constitutiva e inseparable de la misma; Art. 2.- En concordancia con el artículo precedente, se deroga parcialmente la Orden de Rectorado 2023-103-ESPE-a-1 de 21 de abril de 2023, específicamente en lo relacionado con las Políticas Generales de la Gestión Institucional 2023- 2025; y, todas aquellas órdenes de rectorado que se opongan a la presente. En lo demás, la referida Orden de Rectorado tiene plena vigencia y valor legal, en todo lo que no haya sido derogado por otra orden de rectorado”*

- 1.11. Memorando Nro. ESPE-REC-2023-0897-M de 18 de mayo de 2023, a través del cual el Rector de la Universidad de las Fuerzas Armadas - ESPE, realizó la socialización de la “POLÍTICA ESPECÍFICA PARA LA APLICABILIDAD DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES”

C. DEFINICIONES

1. **Autoridad de Protección de Datos Personales:** Autoridad pública independiente encargada de supervisar la aplicación de la Ley Orgánica de Protección de Datos Personales, reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales.
2. **Anonimización:** La aplicación de medidas dirigidas a impedir la identificación o reidentificación de una persona natural, sin esfuerzos desproporcionados.
3. **Base de datos o fichero:** Conjunto estructurado de datos cualquiera que fuera la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica.
4. **Consentimiento:** Manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos.
5. **Dato biométrico:** Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros.
6. **Dato genético:** Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo.
7. **Dato personal:** Dato que identifica o hace identificable a una persona natural, directa o indirectamente.
8. **Datos personales crediticios:** Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera.
9. **Datos relativos a:** etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos, datos relativos a las personas apátridas y refugiados que requieren protección internacional, y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.
10. **Datos relativos a la salud:** datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.
11. **Datos sensibles:** Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.
12. **Delegado de protección de datos:** Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el

- cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos.
13. **Destinatario:** Persona natural o jurídica que ha sido comunicada con datos personales.
 14. **Elaboración de perfiles:** Todo tratamiento de datos personales que permite evaluar, analizar o predecir aspectos de una persona natural para determinar comportamientos o estándares relativos a: rendimiento profesional, situación económica, salud, preferencias personales, intereses, habilidad, ubicación, movimiento físico de una persona, entre otros.
 15. **Encargado del tratamiento de datos personales:** Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.
 16. **Entidad Certificadora:** Entidad reconocida por la Autoridad de Protección de Datos Personales, que podrá, de manera no exclusiva, proporcionar certificaciones en materia de protección de datos personales.
 17. **Fuente accesible al público:** Bases de datos que pueden ser consultadas por cualquier persona, cuyo acceso es público, incondicional y generalizado.
 18. **Responsable de tratamiento de datos personales:** persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales.
 19. **Sellos de protección de datos personales:** Acreditación que otorga la entidad certificadora al responsable o al encargado del tratamiento de datos personales, de haber implementado mejores prácticas en sus procesos, con el objetivo de promover la confianza del titular, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.
 20. **Seudonimización:** Tratamiento de datos personales de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional, figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyen a una persona física identificada o identificable.
 21. **Titular:** Persona natural cuyos datos son objeto de tratamiento.
 22. **Transferencia o comunicación:** Manifestación, declaración, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales. Los datos personales que comunique deben ser exactos, completos y actualizados.
 23. **Tratamiento:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.
 24. **Vulneración de la seguridad de los datos personales:** Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales.

D. PRINCIPIOS

La Universidad de las Fuerzas Armadas - ESPE, en cumplimiento con lo establecido en la Ley Orgánica de Protección de Datos Personales, reconoce y garantiza el derecho fundamental a la protección de los datos personales, el cual incluye tanto el acceso a la información como la toma de decisiones sobre la misma. Además, asegura su resguardo adecuado, por lo que el tratamiento de los datos personales de los titulares se llevará a cabo conforme a la legalidad, con el consentimiento explícito del titular y, cuando corresponda, bajo las directrices proporcionadas por los responsables del tratamiento.

En el manejo de datos personales, la Universidad implementará los principios establecidos en la Ley Orgánica de Protección de Datos Personales y su reglamento, aplicándolos de acuerdo con su política interna. Los principales principios que guiarán dicho tratamiento incluyen:

1. **Juridicidad:** Los datos personales se procesarán de manera estricta y conforme a los principios, derechos y obligaciones previstos en la Constitución, los tratados internacionales ratificados, la Ley Orgánica de Protección de Datos Personales, su reglamento y la normativa y jurisprudencia vigente.
2. **Lealtad:** El tratamiento de los datos personales deberá realizarse de manera leal, asegurando que los titulares sean claramente informados sobre la recolección, uso, consulta o cualquier otro tipo de tratamiento de sus datos. En ningún caso los datos podrán ser utilizados para fines ilícitos o desleales.
3. **Transparencia:** El tratamiento de los datos debe ser transparente, lo que implica que la información relacionada con este proceso debe ser fácilmente accesible, comprensible y presentada en un lenguaje claro y sencillo. Todas las relaciones derivadas del tratamiento de datos se registrarán por las disposiciones de la Ley Orgánica de Protección de Datos Personales y su reglamento.
4. **Finalidad:** Los datos personales sólo se tratarán para fines previamente determinados, explícitos y legítimos, que serán comunicados al titular. En ningún caso los datos podrán ser utilizados para finalidades distintas a las inicialmente informadas, salvo que existan causas legales que justifiquen un nuevo tratamiento, conforme a los principios de tratamiento legítimo establecidos en la ley. Si los datos personales son tratados para fines distintos a aquellos para los cuales fueron recopilados, este nuevo tratamiento solo será permitido si es compatible con los fines originales de recolección. Esto debe considerar el contexto en que se recabaron los datos, la información proporcionada al titular en ese proceso y las expectativas razonables del titular.
5. **Pertinencia y minimización de datos:** Los datos personales deben ser pertinentes y limitados a lo estrictamente necesario para cumplir con el fin para el cual fueron recolectados.
6. **Proporcionalidad:** El tratamiento de los datos personales debe ser adecuado, necesario, oportuno, relevante y no excesivo en relación con las finalidades para las que se recolectaron o con la naturaleza de las categorías de datos.
7. **Confidencialidad:** Los datos personales deben ser tratados con la máxima confidencialidad, garantizando que no se comuniquen ni se utilicen para fines distintos a aquellos para los cuales fueron recolectados, a menos que existan causas legales que permitan un nuevo tratamiento. El responsable del tratamiento deberá adoptar medidas técnicas y organizativas adecuadas para asegurar este principio.
8. **Calidad y exactitud:** Los datos personales tratados deben ser exactos, completos, actualizados y verificables. Se adoptarán todas las medidas razonables para corregir o suprimir cualquier dato incorrecto sin demora, de acuerdo con los fines para los cuales fueron recolectados. En caso de que el tratamiento sea realizado por un encargado, será responsabilidad del responsable garantizar la exactitud de los datos.
9. **Conservación:** Los datos personales serán conservados durante el tiempo necesario para cumplir con la finalidad del tratamiento. El responsable establecerá plazos de conservación, revisándolos periódicamente, y los datos sólo se conservarán más allá de este plazo si es necesario para fines archivísticos, científicos, históricos o estadísticos, siempre con las garantías de seguridad necesarias.

10. Seguridad de los datos personales: El responsable y los encargados del tratamiento deberán implementar medidas de seguridad adecuadas para proteger los datos personales frente a riesgos, amenazas o vulnerabilidades, de acuerdo con la naturaleza de los datos, el ámbito y el contexto en que se procesan. Estas medidas pueden ser organizativas, técnicas u otras apropiadas.
11. Responsabilidad proactiva: El responsable del tratamiento deberá demostrar que ha implementado mecanismos efectivos para proteger los datos personales, cumpliendo con los principios y obligaciones establecidos por la Ley Orgánica de Protección de Datos Personales. Esto incluye la utilización de estándares, mejores prácticas, esquemas de autorregulación, certificaciones o cualquier otro mecanismo pertinente.
12. Aplicación favorable al titular: En caso de duda sobre el alcance de las disposiciones legales o contractuales aplicables a la protección de datos personales, los funcionarios judiciales y administrativos deberán interpretarlas y aplicarlas de la manera más favorable al titular de los datos.
13. Independencia del control: Para asegurar el efectivo ejercicio del derecho a la protección de datos personales y el cumplimiento de las obligaciones del Estado en esta materia, la Autoridad de Protección de Datos deberá actuar de forma independiente, imparcial y autónoma, realizando las acciones necesarias de prevención, investigación y sanción, según corresponda.

E. DECLARACIÓN ESTATUTARIA

La Universidad de las Fuerzas Armadas - ESPE, es una institución de educación superior con personería jurídica, de derecho público y sin fines de lucro; con autonomía académica, administrativa, financiera, orgánica y patrimonio propio. Como institución de educación superior de las Fuerzas Armadas es dependiente del Comando Conjunto de las Fuerzas Armadas en política institucional en el ámbito de la educación superior, designación de autoridades; y asignación del personal militar necesario para su funcionamiento.

F. ÁMBITO DE APLICACIÓN

La Política de Protección de Datos Personales se aplicará en la Universidad de las Fuerzas Armadas - ESPE: Matriz (campus Sangolquí), Sede Latacunga (campus General de División Guillermo Rodríguez Lara y campus Centro), Sede Santo Domingo de los Tsáchilas, Centros, y Unidades Académicas Especiales, así como a toda sede o estructura que se creará a futuro como dependencia de la universidad; a todo dato personal que sea tratado, a través de los diferentes medios digitales y físicos, dentro y fuera del territorio nacional.

G. LINEAMIENTOS GENERALES PARA EL TRATAMIENTO DE DATOS PERSONALES

Obligaciones y Responsabilidades de la Universidad como Responsable del Tratamiento de Datos Personales

La Universidad de las Fuerzas Armadas - ESPE es una entidad de educación superior cuyas funciones sustantivas son la docencia, investigación y vinculación con la sociedad, apoyadas por procesos; en virtud de lo cual tratará los datos personales en lo siguiente:

1. Prestar servicios y asistencia solicitados por los usuarios.
2. Gestionar y almacenar la información de estudiantes, personal administrativo, personal académico, proveedores, terceros y cualquier persona natural o jurídica que tenga relación actual o potencial con la Universidad, acorde a la normativa vigente.
3. Proporcionar información sobre programas académicos, carreras universitarias, posgrados, talleres, cursos y charlas en modalidad presencial o virtual.
4. Dar atención a las solicitudes de información relacionadas con las competencias institucionales.
5. Dar a conocer nuevos proyectos, productos y servicios ofrecidos por la institución.
6. Contactar a usuarios que hayan aceptado la política de privacidad, incluyendo la confirmación de la información proporcionada.

7. Utilizar la información, previa autorización, para prevenir actividades ilícitas, garantizar el cumplimiento de términos y condiciones, y aplicar medidas disciplinarias cuando corresponda. Bajo este ámbito también se emplearán herramientas tecnológicas para detectar actividades anómalas como el spam.
8. Evaluar y mejorar los servicios y productos de la universidad mediante la retroalimentación del usuario a través de encuestas, grupos de enfoque u otros métodos estadísticos.
9. Facilitar la interacción de los usuarios a través de foros en línea, redes sociales y otros servicios que permitan publicar comentarios, opiniones y contenido.
10. Gestionar transacciones que requieran el uso de información personal, como nombre, dirección, correo electrónico, datos financieros y medios de pago, para garantizar la prestación adecuada de servicios universitarios.
11. Compartir información sobre oportunidades laborales disponibles en la bolsa de empleo institucional, basada en los datos académicos y profesionales proporcionados por el Titular.
12. Evaluar y rastrear el uso de los servicios universitarios, a través de estadísticas internas, para comprender mejor su nivel de utilización.
13. Proveer información sobre servicios y beneficios destinados a graduados.
14. Difundir noticias, eventos, investigaciones y programas institucionales relacionados con áreas académicas, vinculación con la sociedad, investigación, y otras relacionadas con la universidad.
15. Atender inquietudes, responder solicitudes y fomentar la participación en programas y proyectos de investigación.
16. Compartir información laboral y académica, y suscribir convenios, contratos con entidades nacionales e internacionales para el posicionamiento en rankings y acreditaciones.
17. Suscribir convenios de cooperación con entidades externas.
18. Brindar a las personas el derecho a conocer qué información se tiene sobre ellas, a solicitar la corrección o eliminación de datos erróneos o innecesarios, y a oponerse al tratamiento de sus datos en determinadas circunstancias.
19. Crear un entorno de confianza en el que las personas puedan compartir sus datos personales con la seguridad de que serán tratados de manera adecuada y respetuosa.
20. Evitar la divulgación de información personal que pueda dañar la reputación de una persona.
21. Prevenir fraudes y el robo de identidad.
22. Implementar medidas de seguridad relacionadas al control de accesos a la Universidad.
23. Realizar el control de asistencia del personal que tiene relación de dependencia con la Universidad.
24. Tratar datos personales en estricto apego a los principios y derechos desarrollados en la Ley Orgánica de Protección de Datos Personales, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;
25. Aplicar e implementar requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la Ley Orgánica de Protección de Datos Personales, su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;
26. Aplicar e implementar procesos de verificación, evaluación, valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas;
27. Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular;
28. Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;
29. Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales;
30. Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;
31. Notificar a la Autoridad de Protección de Datos Personales y al titular de los datos acerca de violaciones a las seguridades implementadas para el tratamiento de datos personales conforme a lo establecido en el procedimiento previsto para el efecto;

32. Implementar la protección de datos personales desde el diseño y por defecto;
33. Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;
34. Asegurar que el encargado del tratamiento de datos personales ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme a lo establecido en la Ley Orgánica de Protección de Datos Personales, su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, normativa sobre la materia y las mejores prácticas a nivel nacional o internacional;
35. Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales, de conformidad a lo dispuesto en la Ley, su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales;
36. Designar al Delegado de Protección de Datos Personales;
37. Permitir y contribuir a la realización de auditorías o inspecciones, por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales.
38. El encargado de tratamiento de datos personales tendrá las mismas obligaciones que el responsable de tratamiento de datos personales, en lo que sea aplicable, de acuerdo a la Ley Orgánica de Protección de Datos Personales y su reglamento;
39. Los demás establecidos en la Ley Orgánica de Protección de Datos Personales, su reglamento, en directrices, lineamientos, regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

Valoración de Riesgos en el Tratamiento de Datos Personales

La Universidad de las Fuerzas Armadas - ESPE podrá llevar a cabo una evaluación de impacto en el tratamiento de datos personales cuando se determine que dicho tratamiento (debido a su naturaleza, contexto o fines) presenta un alto riesgo para los derechos y libertades de los titulares de los datos. Asimismo, esta evaluación será realizada si así lo requiere la Autoridad de Protección de Datos Personales.

La Autoridad de Protección de Datos Personales podrá identificar situaciones de tratamiento que requieran la realización de una evaluación en el tratamiento de datos.

Legitimidad del Tratamiento de Datos Personales

De acuerdo con lo establecido en la Ley Orgánica de Protección de Datos Personales, el tratamiento de datos personales es considerado legítimo y conforme a la ley cuando se cumple con alguna de las siguientes condiciones:

14. Consentimiento del Titular: El tratamiento se realiza con el consentimiento explícito del titular de los datos para fines específicos, ya sea uno o varios, de acuerdo con lo previamente informado.
15. Cumplimiento de Obligación Legal: El tratamiento se lleva a cabo por parte del responsable del tratamiento para dar cumplimiento a una obligación legal que le corresponde.
16. Orden Judicial: El tratamiento se efectúa a solicitud de una autoridad judicial competente, respetando siempre los principios establecidos en la Ley Orgánica de Protección de Datos Personales.
17. Interés Público o Ejercicio de Poderes Públicos: El tratamiento es necesario para cumplir con una misión de interés público o para el ejercicio de funciones y poderes públicos otorgados al responsable, siempre que se respete la legalidad, proporcionalidad y necesidad, y se garanticen los derechos humanos de los titulares.
18. Medidas Precontractuales y Contractuales: El tratamiento se realiza con el propósito de ejecutar medidas precontractuales solicitadas por el titular, o para cumplir con obligaciones derivadas de un contrato en el que el responsable del tratamiento o un tercero legalmente autorizado sea parte.

19. Protección de Intereses Vitales: El tratamiento es necesario para proteger intereses vitales del titular o de otra persona, como su vida, salud o integridad física o psicológica.
20. Datos en Bases de Datos Públicas: El tratamiento de datos personales que estén contenidos en bases de datos accesibles públicamente, conforme a lo establecido por la normativa aplicable.
21. Intereses Legítimos: El tratamiento se realiza para satisfacer un interés legítimo del responsable del tratamiento o de un tercero, siempre y cuando dicho interés no sea superado por los derechos y libertades fundamentales del titular, conforme a las disposiciones de la Ley Orgánica de Protección de Datos Personales.

Plazo de Conservación de Datos Personales

Se establece un período de conservación de 10 años para los datos personales, salvo en el caso de los datos derivados de videovigilancia, cuya conservación será hasta 3 meses. En cuanto al personal docente, administrativo y a los estudiantes, los datos personales serán conservados durante 10 años a partir de su desvinculación de la institución. Finalizado el mismo, se procederá a la eliminación de los datos personales tan pronto como se hayan cumplido todas las acciones necesarias para gestionar y dar por finalizadas las posibles obligaciones pendientes entre las partes, llevando a cabo durante este período las gestiones administrativas pertinentes.

No obstante lo anterior, los datos podrán ser conservados de forma anonimizada para el cumplimiento de otras obligaciones legales que correspondan a la Universidad, así como para fines archivísticos de interés público, o con fines de investigación científica, histórica o estadística.

La Universidad garantiza que dichos datos no serán tratados, salvo en los casos en que sea estrictamente necesario para la formulación, ejercicio o defensa de reclamaciones, o cuando medie una orden judicial o requerimiento de autoridad competente, en cumplimiento de la normativa vigente en materia de protección de datos personales.

Confidencialidad de la Información

La Universidad de las Fuerzas Armadas - ESPE, se compromete a tratar toda la información proporcionada de manera voluntaria con la más estricta confidencialidad, respetando en todo momento las garantías y medidas de seguridad establecidas por la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales, su reglamento y la normativa vigente aplicable. Esta información será utilizada exclusivamente por la Universidad de las Fuerzas Armadas - ESPE para los fines especificados en el presente documento.

De manera excepcional, la Universidad podrá compartir la información con terceros autorizados por ley que colaboren en la ejecución de actividades descritas en este documento, siempre y cuando dicha divulgación se limite a cumplir con los fines establecidos. En todos los casos, se tomarán las medidas necesarias para garantizar que la seguridad de la información no se vea comprometida.

Sin perjuicio de lo anterior, la Universidad no será responsable por el tratamiento posterior o uso indebido que el tercero haga de los datos personales entregados, cuando dicho tratamiento exceda o contravenga los fines expresamente autorizados por la Universidad o por el titular de los datos. En tales casos, será el tercero quien asumirá la responsabilidad correspondiente conforme al régimen sancionatorio previsto en la Ley Orgánica de Protección de Datos Personales.

La Universidad de las Fuerzas Armadas - ESPE no vende ni cede a terceros los datos personales que recibe. Los datos proporcionados serán tratados con total confidencialidad. Para garantizar su protección, se adoptarán los niveles de seguridad requeridos por la legislación y se implementarán las medidas técnicas y organizativas

pertinentes para prevenir la pérdida, el uso indebido, la alteración, el acceso no autorizado o el robo de datos personales.

Finalidades del Tratamiento de Datos Personales

En cumplimiento con la Ley Orgánica de Protección de Datos Personales, la Universidad de las Fuerzas Armadas - ESPE realiza diversas actividades de tratamiento sobre la información personal proporcionada por sus titulares, a través de sus distintos canales de atención y en formatos tanto físicos como electrónicos. Estos procesos incluyen la recolección, registro, organización, almacenamiento, conservación, adaptación, modificación, eliminación, extracción, consulta, distribución, cesión, comunicación, transferencia, supresión y destrucción de la información, que es integrada en las bases de datos o repositorios de la Universidad, ya sea de manera directa o a través de terceros.

La información recolectada tiene como fin su utilización en el ejercicio de las funciones propias de la Universidad como institución de educación superior, conforme al Registro de Actividades de Tratamiento (RAT).

Destinatarios a Terceros de Datos Personales

En cumplimiento de la normativa y los requerimientos establecidos por los entes rectores de la educación superior, los datos personales de los miembros de la comunidad universitaria podrán ser transferidos, de manera parcial, a entidades externas autorizadas por ley como: Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT), Sistema Nacional de Información de Educación Superior del Ecuador (SNIESE), Ministerio de Trabajo, Servicio de Rentas Internas, entre otros.

No obstante de lo indicado, los datos personales serán compartidos con terceros únicamente cuando:

1. Así lo exija la normativa vigente o la autoridad competente, o
2. Cuando se haya obtenido previamente la autorización correspondiente.

La transferencia de datos se realizará tras la suscripción de la autorización para el tratamiento de datos personales del titular, a menos que se hayan dissociado los datos, el cual puede ser revocado en cualquier momento ante el responsable del tratamiento, quien a su vez deberá notificar al tercero destinatario de la comunicación de datos personales para que proceda con la rectificación, actualización, oposición o eliminación, según sea el caso. Además se garantizará que solo se proporcione la información estrictamente necesaria para llevar a cabo las actividades autorizadas por el Responsable del Tratamiento de Datos Personales.

Registro y uso de cookies en sitios web

La Universidad de las Fuerzas Armadas - ESPE utiliza cookies y registra automáticamente información de navegación para mejorar la calidad de los servicios web y garantizar la funcionalidad de sus sistemas informáticos.

Dado que las cookies se almacenan en los navegadores web, es a través de estos que el Titular puede ejercer su derecho a desactivarlas o eliminarlas. No obstante, es importante señalar que la Universidad de las Fuerzas Armadas - ESPE no puede garantizar la correcta o incorrecta manipulación de las cookies realizada por dichos navegadores web.

Sin embargo, en la Universidad se realiza un seguimiento de los sitios web visitados y se mide el tiempo de uso de los sistemas informáticos, para ello los datos recopilados incluyen:

1. Comportamiento de navegación en el sitio web.
2. Ubicación geográfica.
3. Dispositivo y navegador utilizado.
4. Fecha y hora de solicitudes al servidor.

La información es utilizada para fines estadísticos, académicos, laborales, contractuales, disciplinarios, de investigación, innovación, vinculación, rankings, acreditaciones, seguridad de la información y mejoras en los portales web, entre otros.

Derechos de los Titulares.

Los titulares de los datos personales podrán ejercer, entre otros, los siguientes derechos frente a la Universidad en su rol de Responsable y/o Encargado del tratamiento de la información:

22. Derecho a la información.- El titular de datos personales tiene derecho a ser informado conforme los principios de lealtad y transparencia, de cualquier modo comprobable en lenguaje claro, sencillo y de fácil comprensión, sobre el tratamiento de sus datos personales.
23. Derecho de acceso.- El titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento, acceso a todos sus datos personales y su tratamiento, sin necesidad de presentar justificación alguna.
24. Derecho de rectificación, actualización y eliminación.- El titular tiene el derecho a obtener del responsable del tratamiento, la rectificación y actualización y eliminación de sus datos personales inexactos o incompletos.
25. Derecho de oposición.- El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en los casos establecidos en la Ley Orgánica de Protección de Datos Personales.
26. Derecho a la portabilidad.- El titular tiene el derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características; o a transmitirlos a otros responsables, en los casos establecidos en la Ley Orgánica de Protección de Datos Personales. La Autoridad de Protección de Datos Personales deberá dictar la normativa para el ejercicio al derecho de la Portabilidad.
27. Derecho a la suspensión del tratamiento.- El titular tendrá derecho a obtener del responsable del tratamiento la suspensión del tratamiento de los datos cuando se cumpla alguna de las condiciones establecidas en la Ley Orgánica de Protección de Datos Personales.
28. Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas.- El titular tiene derecho a no ser sometido a una decisión basada única o parcialmente en valoraciones que sean producto de procesos automatizados, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o que atenten contra sus derechos y libertades fundamentales.
29. Derecho de consulta.- Las personas tienen derecho a la consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales, de conformidad con la Ley Orgánica de Protección de Datos Personales

El Titular o su representante legal podrá ejercer sus derechos en cualquier momento y de manera gratuita, a la autorización del tratamiento de sus datos personales previamente realizada. Para ello, se podrá descargar y completar adecuadamente el ANEXO A (Formulario para el ejercicio de los derechos de protección de datos personales), y presentar su solicitud a la Universidad de las Fuerzas Armadas - ESPE de manera física o a través del siguiente canal virtual:

Correo Electrónico:

datos-personales@espe.edu.ec

Horario de Atención:

7h00 a 16h00

Es importante tener en cuenta que, para realizar el trámite, el Titular debe acreditar su identidad como Titular de los datos o como representante legal debidamente autorizado.

Una vez recibida y validada la solicitud, la Universidad de las Fuerzas Armadas - ESPE se comunicará directamente con el Titular o su representante legal para informar sobre el estado del trámite y las acciones correspondientes.

Medidas para precautelar la seguridad de los datos personales

Todas las unidades de la Universidad de las Fuerzas Armadas - ESPE tienen la responsabilidad de salvaguardar la confidencialidad, integridad y disponibilidad de la información, cumpliendo con los procedimientos establecidos en la normativa de protección de datos personales; esto incluye un enfoque particular de la gestión y protección de la información que reposa en los sistemas informáticos y aplicativos de la Universidad, así como de aquellos procesos que involucren el manejo de datos personales sensibles.

Es importante destacar que el suministro de datos inexactos por parte del Titular puede impedir total o parcialmente el cumplimiento de la finalidad para la cual fueron recopilados.

La Universidad notificará a la comunidad universitaria y a los visitantes sobre la presencia de cámaras de seguridad para videovigilancia a través de avisos ubicados en lugares visibles. Las grabaciones obtenidas por estas cámaras se utilizarán exclusivamente como pruebas en procesos administrativos o judiciales, ante la solicitud de las autoridades competentes.

En su calidad de responsable del tratamiento de datos personales, la Universidad está obligada a rendir cuentas tanto a los titulares de los datos como a la Autoridad de Protección de Datos Personales.

La Universidad implementará un proceso de supervisión, evaluación y análisis continuo de la eficacia, eficiencia y efectividad de las medidas técnicas y organizativas adoptadas, con el fin de garantizar y mejorar la seguridad en el tratamiento de los datos personales. Asimismo, se asegurará de que las medidas implementadas sean suficientes para mitigar adecuadamente los riesgos identificados. Además, se tomarán las medidas necesarias para garantizar que, por defecto, sólo se procesen los datos personales que sean estrictamente necesarios para cada propósito de tratamiento, conforme a lo estipulado en la Ley Orgánica de Protección de Datos Personales y su Reglamento

La Universidad adoptará de manera continua y permanente las medidas necesarias para identificar, evaluar, prevenir, mitigar y controlar los riesgos, amenazas y vulnerabilidades, incluidas aquellas que puedan representar un alto riesgo para los derechos y libertades de los titulares. Todo ello, en cumplimiento con la normativa que emita la Autoridad competente

H. ROLES DE LA PROTECCIÓN DE DATOS PERSONALES

La gestión de datos personales dentro de la Universidad de las Fuerzas Armadas - ESPE, tendrá los siguientes roles específicos:

1. Titular de datos personales: Persona natural cuyos datos personales son objeto de tratamiento. El Titular tiene derechos sobre el acceso, modificación, rectificación, eliminación y oposición al tratamiento de sus datos personales. En resumen es cualquier miembro de la comunidad universitaria.

2. Responsable del tratamiento de datos personales: Corresponde a quien decide sobre la finalidad, medios y condiciones del tratamiento de los datos personales. La Universidad de las Fuerzas Armadas - ESPE está representada por el Rector.
3. Comité de Seguridad de la Información: Órgano colegiado nombrado por la máxima autoridad de la Universidad, que será el encargado de apoyar la implementación de controles y realizar el seguimiento correspondiente. El Comité de Seguridad de la Información está representado por el Vicerrector Académico General.
4. Delegado de protección de datos personales - DPO: Persona natural designada por la máxima autoridad para asesorar, velar y supervisar de manera independiente, el cumplimiento de las obligaciones legales al responsable y al encargado del tratamiento de datos personales y garantizar el cumplimiento de la ley. Actúa como punto de contacto con las autoridades de control y los titulares de los datos. La designación y perfil de este rol debe cumplir con lo establecido en la normativa vigente.

El delegado de protección de datos personales desempeñará sus funciones de manera profesional, con total independencia del responsable y del encargado del tratamiento de datos personales, quienes estarán obligados a facilitar la asistencia, recursos y elementos que les sea oportunamente requeridos para garantizar el cumplimiento de los deberes, funciones y responsabilidades a cargo del delegado.

El delegado de protección de datos personales podrá ser contratado por el responsable del tratamiento de datos personales, bajo la figura de:

- Relación de Dependencia
- Contrato de Prestación de Servicios Profesionales

En cualquiera de los dos casos, deberá respetar y garantizar que se presten los servicios de manera independiente.

5. Encargado del tratamiento de datos personales: Persona natural o jurídica que trata los datos personales por cuenta del Responsable o Corresponsables del tratamiento, conforme a las instrucciones que éste le proporciona. El/los encargado/s es/son designado/s por el Responsable del tratamiento de Datos Personales, y no decide sobre la finalidad ni sobre los medios del tratamiento. Cabe indicar que es posible realizar el Encargo del Tratamiento de Datos Personales a un ente externo a la Universidad, siempre y cuando se cumpla lo previsto en la normativa vigente.
6. Coordinador del tratamiento de datos personales: Personas designadas al interior de la Universidad por la máxima autoridad, quienes serán los responsables operativos de la gestión de datos personales dentro de las Unidades, Departamentos o Coordinaciones. Puede ser cualquier funcionario que tenga conocimiento sobre los procesos operativos, tecnológicos y/o normativos de datos personales que se tratan en Matriz / Sede / Unidad / Departamento, y estarán bajo la dirección, en el levantamiento y ejecución de procesos, del Delegado de Protección de Datos Personales. Las atribuciones y responsabilidades del Coordinador del tratamiento de datos personales, estarán establecidas en el instructivo que se elaborará para tal fin.

Se levantarán los formatos necesarios para la suscripción de los consentimientos informados (Autorizaciones), y los acuerdos de confidencialidad correspondientes, según el rol asignado a cada actor. La aceptación de estos documentos se llevará a cabo de manera expresa, a través de los medios electrónicos o físicos implementados por la Universidad

I. RESPONSABILIDAD EN EL MANEJO DE DATOS PERSONALES

En el contexto de la relación laboral, académica, de prestación de servicios o contractual con la Universidad, el usuario que acceda a datos personales se compromete a:

1. Utilizar las bases de datos o la información personal a la que pueda tener acceso, ya sea directa o indirectamente, exclusivamente para los fines establecidos por la Universidad.
2. Mantener la confidencialidad en el tratamiento de las bases de datos y los datos personales, incluso después de finalizar su relación con la Universidad.
3. Devolver o destruir la información relativa a bases de datos o datos personales que haya recibido de la Universidad, según las instrucciones que esta última disponga.

En caso de incumplir este compromiso o las disposiciones contenidas en la Ley Orgánica de Protección de Datos Personales y su reglamento, la Universidad podrá adoptar las medidas correctivas pertinentes, sin perjuicio de la posibilidad de iniciar acciones legales, civiles o penales, con el fin de obtener la reparación por los daños y perjuicios causados.

Los usuarios, colaboradores, proveedores o cualquier tercero que mantengan una relación directa o indirecta con la Universidad deberán abstenerse de realizar cualquier actividad o proyecto que implique el uso del nombre, enseña comercial, razón social, símbolos, logotipos, marcas o cualquier otro distintivo de la Institución, sin contar con la autorización previa y por escrito de la Universidad, especialmente si dicha actividad implica el tratamiento de datos personales. Cualquier iniciativa que se lleve a cabo sin cumplir con este requisito será de exclusiva responsabilidad de los autores o promotores y no generará obligaciones ni responsabilidades para la Universidad.

J. ANEXO

[Formulario para el ejercicio de derecho de protección de datos personales](#)

K. CONTROL DE CAMBIOS

Fecha	Versión	Funcionario	Cambio
27/04/2023	1.0	Unidad de Seguridad Integrada	Política Específica para la aplicabilidad de la Ley de Protección de Datos Personales
16/12/2024	2.0	Ab. Maria Augusta de la Torre - USGN Tcnl. (SP) David Molina - USIN / DPO Ing. Magaly Reascos - UTIC Ing. Andrés Castillo - UTIC Ab. Xavier Erazo- UAJR Ing. René Abad - USIN	Revisión previa a que el documento suba a conocimiento del Comité de Seguridad de la Información (Sesión Nro. ESPE-CSI-CSO-2024-002)
18/12/2024	3.0	Cnrl. E.M. Henry Omar Cruz Carrillo, PhD.	Aprobación del documento por el Comité de Seguridad de la Información (Sesión Nro. ESPE-CSI-CSO-2024-002)
02/04/2024 al 07/04/2025		Dra. Ximena Espinosa - UAJR Ing. René Abad - USIN	Revisión requerida por el Rectorado

 ESPE <small>UNIVERSIDAD DE LAS FUERZAS ARMADAS</small> <small>INNOVACIÓN PARA LA EXCELENCIA</small>	POLÍTICA ESPECÍFICA DE PROTECCIÓN DE DATOS PERSONALES DE LA UNIVERSIDAD DE FUERZAS ARMADAS - ESPE	Vicerrectorado Académico General Vicerrectorado Administrativo Unidad de Asesoría Jurídica Unidad de Seguridad Integrada
		Página: 18 de 19

Fecha	Versión	Funcionario	Cambio
28/04/2025	3.0	Crnl. (SP) Miguel Ángel Peña - USIN / DPO Dr. Mauricio Jaramillo - UAJR Dra. Ximena Espinosa - UAJR Dra. Tatiana Gualotuña - VAG Ab.Maria Augusta de la Torre - USGN Ing. Magali Reascos - UTIC Ing. Francisco León - UPDI Ing. René Abad - USIN	Revisión conjunta con el DPO, VAG
29/06/2025		Ab. Melanee Auz - Rectorado	Revisión del documento.

L. APROBACIÓN

Rubro	Nombre	Unidad / Cargo	Firma
Elaborado por:	Dra. Ximena Beatriz Espinosa Barrera	Coordinación General Jurídica / Analista de Asesoría Jurídica	
	Ing. Magali Soraya Reascos Llumiquinga, Mgtr.	Unidad de Tecnologías de la Información y Comunicaciones / Especialista de Provisión de Servicios de TI	
	Ing. René Fernando Abad Jiménez, Mgtr.	Unidad de Seguridad Integrada / Especialista de Seguridad de la Información	
Revisado por:	Crnl. (SP) Carlos Fabián Sarango Erazo	Unidad de Planificación y Desarrollo Institucional Director	
	Crnl. (SP) Miguel Ángel Peña Caguana, Mgtr.	Unidad de Seguridad Integrada / Director - Delegado de Protección de Datos Personales	
	CPFG. Joseph Alexander Guamán Seis, PhD.	Unidad de Tecnologías de la Información y Comunicaciones / Director	

	POLÍTICA ESPECÍFICA DE PROTECCIÓN DE DATOS PERSONALES DE LA UNIVERSIDAD DE FUERZAS ARMADAS - ESPE	Vicerrectorado Académico General Vicerrectorado Administrativo Unidad de Asesoría Jurídica Unidad de Seguridad Integrada
		Página: 19 de 19

Rubro	Nombre	Unidad / Cargo	Firma
	Ab. María Augusta De la Torre Phuma	Unidad de Secretaría General / Secretaría General	
	Dr. José Mauricio Jaramillo Velasteguí, Esp.	Unidad de Asesoría Jurídica / Coordinador Jurídico	
Supervisado por:	CPFG. Joseph Alexander Guamán Seis, PhD.	Vicerrector de Investigación, Innovación y Transferencia de Tecnología / Vicerrector	
	CrnI. C.S.M. Edison Eduardo Haro Albuja, PhD.	Vicerrector de Docencia	
	CPNV José Luis Troya Andrade, Mgtr.	Vicerrector Administrativo	
	CrnI. E.CIV.Enrique Abel Morales Moncayo	Vicerrector Académico General Subrogante	
Aprobado por:	CrnI. C.S.M. Víctor Villavicencio Álvarez, PhD	Rector	