



SECURESOFT

PROCEDIMIENTO DE DERECHO ARCO

Código:	LOPDP-PRO-02
Versión:	0.0
Fecha de la versión:	09-06-2026
Elaborado por:	Implementadora Protección de Datos Personales (PDP)
Revisado por:	Solange Solano Henry Guano Angie Montenegro
Aprobado por:	Patricia Alejandra Falconí Castillo
Nivel de confidencialidad:	Público
ISO 27001	A.5.34
ISO 9001	N/A

CONTENIDO

1. OBJETIVO:.....	4
2. ALCANCE:	4
3. RESPONSABLE DEL PROCESO / RESPONSABLE OPERATIVO	5
4. REFERENCIA NORMATIVA.....	6
4.1 GENERALES:	6
4.2 ESPECÍFICAS:.....	7
5. TÉRMINOS Y DEFINICIONES:.....	13
6. REFERENCIA A INDICADORES DEL PROCESO	15
7. REFERENCIAS A DOCUMENTOS UTILIZADOS	15
8. REGISTROS:	15
9. DIAGRAMA DE FLUJO.....	16

Historial de modificaciones

Fecha	Versión	Descripción del cambio
09-06-2026	0	Versión inicial

1. OBJETIVO:

Establecer un marco claro, transparente y eficaz para la gestión de las solicitudes de los titulares de datos personales que deseen ejercer sus Derechos ARCO+ (Acceso, Rectificación, Cancelación, Oposición, Portabilidad, Limitación del tratamiento, Supresión y a no ser objeto de decisiones individuales automatizadas), en el contexto de las actividades de la **SECURESOFT ECUADOR S.A. (SECURESOFT)**

Este procedimiento tiene como propósito impulsar el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) y su Reglamento General (RGLOPDP).

2. ALCANCE:

Las disposiciones, lineamientos y directrices establecidas en el presente procedimiento son de cumplimiento obligatorio para todo el personal de **SECURESOFT**, incluyendo empleados, directivos, pasantes, contratistas, proveedores y cualquier tercero que preste servicios en nombre de la organización.

Este procedimiento aplica a la totalidad de las actividades de tratamiento de datos personales, ya sean estos físicos o digitales, estructurados o no, que se encuentren bajo la custodia o gestión de **SECURESOFT**, tales como:

2.1 Datos de identificación y contacto:

- Nombres y apellidos
- Número de identificación (cédula, pasaporte u otro documento válido)
- Correo electrónico
- Número de teléfono fijo y/o móvil
- Dirección de domicilio y/o trabajo

2.2 Datos económicos y financieros:

- Datos bancarios
- Información bancaria

2.3 Datos laborales y profesionales:

- Cargo o función

- Empresa o institución a la que pertenece
- Información asociada al perfil profesional

2.4 Datos técnicos y de uso de sistemas:

- Direcciones IP
- Registros de acceso a sistemas (logs)
- Identificadores de dispositivos
- Información generada en el uso de plataformas tecnológicas implementadas o administradas por SECURESOFT.

Este alcance abarca todas las etapas del ciclo de vida del dato: recolección, almacenamiento, uso, transmisión, transferencia, archivo y supresión, dentro de los entornos físicos y digitales de la organización).

3. RESPONSABLE DEL PROCESO / RESPONSABLE OPERATIVO

3.1 Responsable del Tratamiento: SECURESOFT es la responsable legal ante las autoridades de control y los titulares de los datos. Como tal, asume el compromiso de garantizar la implementación de las medidas técnicas y organizativas necesarias para el cumplimiento de la LOPDP y la protección de la información tratada.

3.2 Delegado de Protección de Datos (DPD): Es el garante del cumplimiento normativo interno. Sus funciones principales incluyen:

- Supervisar la correcta aplicación de esta política y del procedimiento de Derechos ARCO+.
- Asesorar a la alta dirección y a las áreas operativas en materia de protección de datos.
- Actuar como punto de contacto oficial con la Superintendencia de Protección de Datos y resolver consultas de los titulares.
- Supervisar la respuesta ante cualquier ejercicio de derechos, asegurando el cumplimiento de los plazos legales.

3.3 Unidades Operativas: Las áreas funcionales (Talento Humano, Comercial, Tecnologías de la Información, Legal, entre otras) actúan como "Custodios Técnicos". Sus responsabilidades son:

- **Ejecución técnica:** Realizar las acciones necesarias (borrado, rectificación, extracción de datos) bajo los estándares de seguridad establecidos.
- **Reporte:** Informar al DPD sobre la finalización de las solicitudes ejecutadas o alertar sobre cualquier complejidad técnica que impida el cumplimiento.
- **Confidencialidad:** Asegurar que todo el personal bajo su cargo mantenga la integridad y confidencialidad de los datos durante el proceso de atención.

4. REFERENCIA NORMATIVA

El presente procedimiento se fundamenta en el marco legal vigente de la República del Ecuador, así como en las mejores prácticas internacionales de seguridad de la información.

- Ley Orgánica de Protección de Datos Personales.
- Reglamento General a la Ley Orgánica de Protección de Datos Personales.
- Resoluciones de la Autoridad de Protección de Datos Personales.
- Constitución de la República del Ecuador.
- Política de Privacidad y Protección de Datos Personales de SECURESOFT ECUADOR S.A.

4.1 GENERALES:

- a) Las directrices establecidas en el presente documento son de observancia obligatoria para todo el personal (empleados, contratistas, pasantes y terceros) involucrado en el ciclo de vida del dato o en la ejecución de actividades de tratamiento dentro de SECURESOFT.
- b) Este procedimiento se rige estrictamente por el ordenamiento jurídico vigente. Ante cualquier vacío normativo o situaciones no previstas en el presente documento, la Dirección o el Comité de Seguridad de la Información (en coordinación con el DPD) emitirá las directrices complementarias necesarias. Dichas instrucciones

tendrán carácter vinculante y permanecerán vigentes hasta que sean formalmente integradas en la siguiente actualización del documento.

- c) SECURESOF asume la responsabilidad integral frente a los titulares por el cumplimiento efectivo del ejercicio de sus derechos ARCO+. La organización garantiza que toda solicitud será gestionada bajo los principios de licitud, lealtad, transparencia y seguridad, abarcando el ejercicio de: Acceso, Rectificación, Cancelación, Oposición, Portabilidad, Limitación del Tratamiento, Supresión y el derecho a no ser objeto de decisiones individuales automatizadas.
- d) La atención de los derechos ARCO+ se regirá bajo criterios de celeridad, gratuidad y eficacia. SECURESOF se compromete a gestionar y resolver toda solicitud dentro de los plazos legales máximos estipulados en la Ley Orgánica de Protección de Datos Personales (LOPD) y su Reglamento General, evitando cualquier dilación injustificada.

4.2 ESPECÍFICAS:

4.2.1 DERECHOS ARCO: Los derechos de los titulares de datos personales se encuentran previstos en la Ley Orgánica de Protección de Datos Personales y su Reglamento. Su ejercicio no es absoluto; por tanto, estará sujeto al cumplimiento de los requisitos, condiciones y excepciones previstos en la normativa vigente para su adecuado ejercicio.

De manera enunciativa más no limitativa, son derechos de los titulares de datos personales:

- a) **Acceso:** El titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales y a la información definida en la Ley Orgánica de Protección de Datos Personales, sin necesidad de presentar justificación alguna.

- b) Rectificación y actualización:** Solicitar la rectificación o actualización de sus datos personales cuando sean inexactos, incompletos o desactualizados.
- c) Eliminación:** Solicitar la eliminación o supresión de sus datos personales cuando:
1. El tratamiento no cumpla con los principios establecidos en la presente Ley.
 2. Los datos no sean necesarios o pertinentes para la finalidad que motivó su tratamiento.
 3. Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados.
 4. Haya vencido el plazo de conservación aplicable.
 5. El tratamiento afecte derechos fundamentales o libertades individuales.
 6. Revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, sin necesidad de que medie justificación alguna.
 7. Exista obligación legal.
- d) Suspensión:** El titular tendrá derecho a obtener del responsable del tratamiento la suspensión del tratamiento de los datos, cuando se cumpla alguna de las condiciones siguientes:
1. Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de estos;
 2. El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
 3. El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.
- e) Portabilidad:** Recibir sus datos personales en un formato compatible, actualizado, estructurado, de uso común, interoperable y lectura mecánica, preservando sus

características; o a transmitirlos a otros responsables del tratamiento cuando sea técnicamente posible.

f) Oposición: El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en los siguientes casos:

1. No se afecten derechos y libertades fundamentales de terceros, la ley se lo permita y no se trate de información pública, de interés público o cuyo tratamiento está ordenado por la ley.
2. El tratamiento de datos personales tenga por objeto la mercadotecnia directa; el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles; en cuyo caso los datos personales dejarán de ser tratados para dichos fines.
3. Cuando no sea necesario su consentimiento para el tratamiento como consecuencia de la concurrencia de un interés legítimo y se justifique en una situación concreta personal del titular, siempre que una ley no disponga lo contrario.

SECURESOFT dejará de tratar los datos personales en estos casos, salvo que acredite motivos legítimos e imperiosos para que el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del titular, o para la formulación, el ejercicio o la defensa de reclamaciones.

g) No ser objeto de decisiones basadas 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.

- h) A la Información:** Ser informado de manera transparente, previa y clara sobre el tratamiento de sus datos personales, conforme a los principios de lealtad y transparencia.
- i) A Revocar su Consentimiento:** En cualquier momento sin que sea necesaria una justificación, el titular podrá revocar el consentimiento otorgado para el tratamiento de sus datos personales. El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos.

4.2.2 DEL PROCEDIMIENTO:

1. Toda solicitud para el ejercicio de derechos ARCO+ deberá ser canalizada exclusivamente a través del correo electrónico oficial: datospersonales@securesoftcorp.com
Cualquier otra vía de comunicación no será considerada como recepción formal del requerimiento.
2. Previo al inicio de cualquier trámite, el Jefe General de Inteligencia de Negocios verificará el cumplimiento de los requisitos mínimos:
 - a. Presentación del documento LOPDP-FOR-02 "Formulario único de ejercicio de derechos ARCO" debidamente completado.
 - b. Copia legible del documento de identidad del titular.
 - c. En caso de actuar mediante apoderado, se deberá adjuntar el documento que acredite la representación legal o poder notariado.
3. En caso de que la solicitud presentada por el titular se encuentre incompleta o no contenga la información necesaria para su adecuada atención, el responsable requerirá al titular que la complete o subsane dentro del término de cinco (5) días contados desde la notificación de dicho requerimiento.
4. Mientras no se proporcione la información solicitada, se suspenderá el cómputo de los plazos legales para la atención de la solicitud, los cuales se reanudarán una vez que el titular haya cumplido con la subsanación requerida.

5. Antes de proceder con la ejecución de cualquier derecho, el responsable y de ser requerido, el Oficial de Seguridad de la Información (OSI), con la asesoría del Delegado de Protección de Datos realizarán una Evaluación de Impacto y Riesgos. Este análisis es mandatorio y debe documentarse, con el objetivo de:
 - a) Validar la identidad del titular para prevenir suplantaciones.
 - b) Evaluar posibles afectaciones a la confidencialidad o integridad de datos de terceros.
 - c) Determinar las medidas técnicas (anonimización, seudonimización o restricciones de acceso) necesarias antes de la ejecución.
6. SECURESOFT se compromete a notificar al titular el resultado de su requerimiento en un plazo máximo de quince (15) días, contados a partir de la recepción y validación completa de la documentación. La respuesta deberá ser motivada, precisa y, en caso de ejecución, detallará las acciones técnicas y administrativas realizadas.
7. Se podrá denegar la solicitud de manera motivada cuando se configure cualquiera de las siguientes causales, notificando al titular mediante correo electrónico:
 - a) Cuando el solicitante no sea el titular de los datos o su representante no esté debidamente acreditado.
 - b) Cuando los datos sean necesarios para el cumplimiento de obligaciones legales, regulatorias, tributarias o contractuales a cargo de SECURESOFT.
 - c) Cuando exista una orden judicial, resolución o mandato motivado de autoridad competente que impida la intervención.
 - d) Cuando la información sea indispensable para la formulación, ejercicio o defensa de acciones judiciales o administrativas.
 - e) Cuando la atención pueda ocasionar perjuicios a derechos o intereses legítimos de terceros, debidamente acreditados.
 - f) Cuando la intervención de los datos obstaculice actuaciones judiciales o administrativas en curso debidamente notificadas.
 - g) Cuando los datos sean necesarios para el ejercicio del derecho a la libertad de expresión y opinión.

- h) Cuando la intervención sea necesaria para proteger el interés vital del titular o de un tercero.
 - i) Cuando medie un interés público, bajo criterios de legalidad, proporcionalidad y necesidad conforme a estándares internacionales.
 - j) Cuando los datos sean necesarios para fines de archivo histórico, estadístico o científico, o constituyan patrimonio del Estado.
- 8. SECURESOF mantendrá un registro centralizado y actualizado de todas las solicitudes de ejercicio de derechos ARCO+, el cual será administrado por el Jefe General de Inteligencia de Negocios, con el apoyo del Oficial de Seguridad de la Información (OSI) y bajo supervisión del Delegado de Protección de Datos Personales.
- 9. Cada solicitud deberá ser registrada en una bitácora oficial, desde el momento de su recepción formal, asignándose un código único de identificación que permita su trazabilidad durante todo el ciclo de atención. La bitácora se registrará conforme el LOPDP-FOR-001 *"Bitácora de registro del Ejercicio de Derechos de Protección de Datos Personales"*.
- 10. El registro deberá reflejar de manera expresa cualquier suspensión de plazos, indicando su causa, fecha de inicio y fecha de reanudación, garantizando así la trazabilidad del cumplimiento de los términos legales.
- 11. Una vez atendida la solicitud, el responsable deberá registrar en la bitácora el cierre del procedimiento, dejando constancia de la respuesta emitida al titular, las acciones ejecutadas y los fundamentos de la decisión adoptada, incluyendo en su caso la motivación de la negativa.
- 12. El expediente de cada solicitud deberá consolidarse en formato físico o digital, incluyendo toda la documentación de respaldo, comunicaciones, evaluaciones de riesgo, validaciones de identidad y evidencias de cumplimiento, garantizando su integridad, autenticidad y disponibilidad.

13. La información contenida en la bitácora y en los expedientes deberá ser conservada por el tiempo necesario para el cumplimiento de obligaciones legales, regulatorias y de control, y podrá ser utilizada como evidencia ante requerimientos de la autoridad competente, auditorías internas o externas.
14. El acceso a la bitácora y a los expedientes estará restringido al personal autorizado, bajo criterios de necesidad y confidencialidad, debiendo aplicarse las medidas de seguridad correspondientes para evitar accesos no autorizados, alteración o pérdida de la información.

5. TÉRMINOS Y DEFINICIONES:

Se establecen las siguientes definiciones para el entendimiento común de las indicaciones del presente documento:

- **Dato personal:** Dato que identifica o hace identificable a una persona natural, directa o indirectamente.
- **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.
- **Titular:** Persona natural cuyos datos son objeto de tratamiento.
- **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.

- **Encargado del tratamiento de datos personales:** Persona natural o jurídica, empresa 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.
- **Acceso no autorizado:** Acceso a información o sistemas sin el permiso adecuado, lo cual puede comprometer la confidencialidad, integridad o disponibilidad de los activos de información.
- **Activos de información:** Todos los datos, documentos, sistemas, aplicaciones, bases de datos y otros elementos digitales o físicos que contienen información relevante para la SECURESOF, y que requieren protección y gestión adecuada.
- **Confidencialidad:** Principio de seguridad que asegura que la información esté accesible únicamente a las personas autorizadas, protegiendo los datos de divulgación no autorizada.
- **Disponibilidad:** Atributo de la información que garantiza que los activos de información estén accesibles y utilizables por los usuarios autorizados cuando sea necesario.
- **Integridad:** Propiedad de la información que garantiza que los datos se mantienen exactos y completos durante todo su ciclo de vida, sin ser alterados de manera indebida.
- **Riesgo de seguridad de la información:** Posibilidad de que ocurran eventos que afecten la confidencialidad, integridad o disponibilidad de los activos de información, lo que podría impactar negativamente las operaciones o la reputación del corporativo.
- **Transparencia organizacional:** Compromiso de la organización con la apertura y claridad en el manejo de la información, promoviendo la confianza y el cumplimiento normativo en todas las áreas.
- **Plazo del requerimiento:** Se entenderá por plazo el período contado en días calendario, que incluye todos los días del mes sin distinción de hábiles o no hábiles.
- **ARCO+:** El concepto ARCO+ se refiere al conjunto de derechos que la LOPDP reconoce a las personas para ejercer control sobre el uso de sus datos personales. Incluye los derechos tradicionales de acceso,

rectificación, cancelación o supresión y oposición, pero se amplía con otros derechos complementarios como la portabilidad, la limitación del tratamiento, la revocación del consentimiento, la posibilidad de no ser objeto de decisiones automatizadas y el derecho a recibir información clara y transparente sobre el tratamiento. En su conjunto, ARCO+ constituye el núcleo de la autodeterminación informativa y garantiza que el titular mantenga poder real y efectivo sobre sus datos personales.

6. REFERENCIA A INDICADORES DEL PROCESO

Nombre del indicador	Objetivo	Fórmula	Frecuencia	Meta	Responsable	Fuente de datos
% de solicitudes ARCO+ atendidas dentro del plazo legal	Asegurar el cumplimiento de los plazos legales de respuesta a los titulares	$\left(\frac{\text{N}^{\circ} \text{ de solicitudes ARCO+ atendidas dentro de los 15 días plazo}}{\text{Total de solicitudes ARCO+ recibidas en el periodo}} \right) \times 100$	Semestral	≥ 95%	Jefe Nacional de Inteligencia de Negocios	Bitácora de Solicitudes de Derechos ARCO+

7. REFERENCIAS A DOCUMENTOS UTILIZADOS

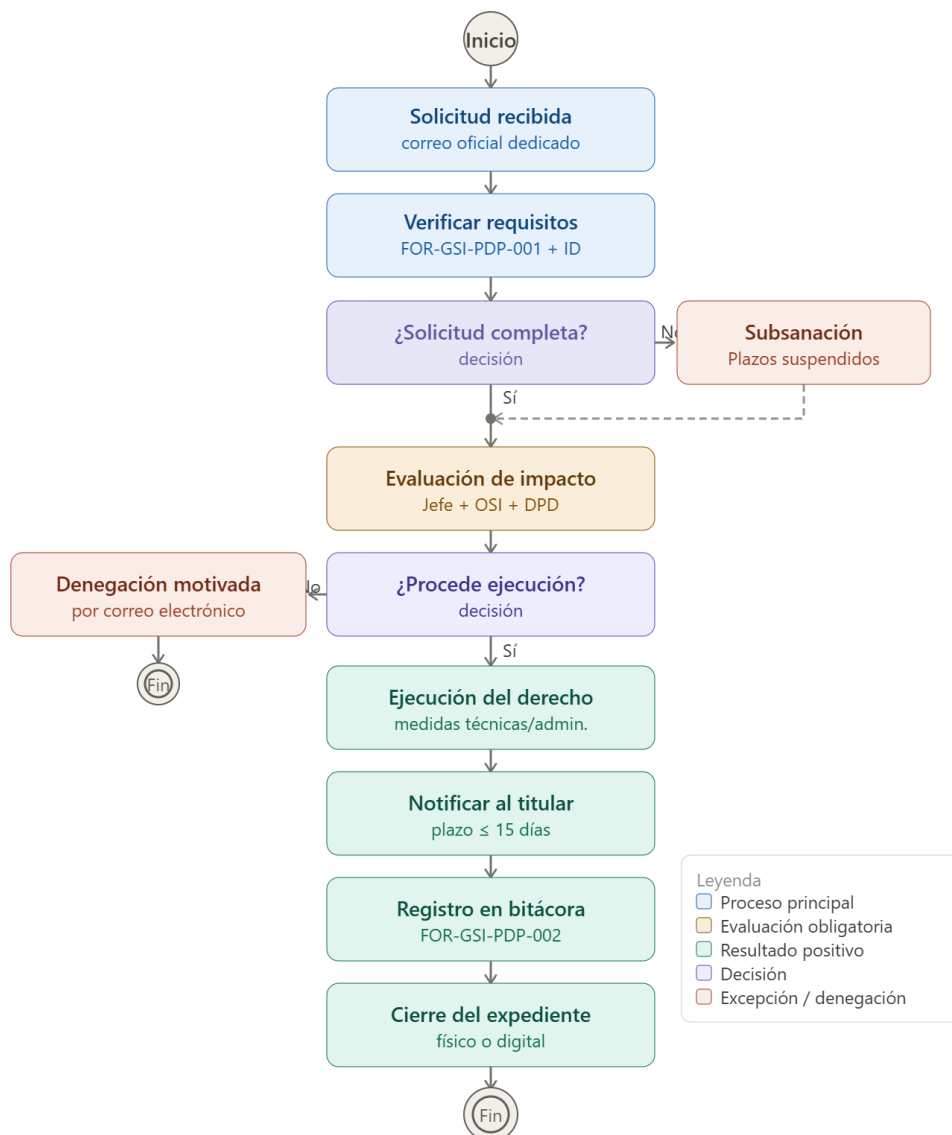
CÓDIGO	NOMBRE
LOPDP-FOR-01	Bitácora de registro de derechos ARCO
LOPDP-FOR-02	Formulario único de derechos ARCO

8. REGISTROS:

REGISTRO	DESCRIPCIÓN	RESPONSABLE OPERATIVO
----------	-------------	-----------------------

LODP-PRO-02 Formulario único de derechos ARCO	Instrumento destinado a estandarizar la presentación de los requerimientos de los titulares, asegurando que cada gestión cumpla con los requisitos formales y documentales establecidos por la normativa aplicable se deberá custodiar en forma cronológica.	Jefe Nacional de Inteligencia de Negocios
LODP-PRO-01 Bitácora de registro de derechos ARCO	Registro manual que permite documentar todas las gestiones relacionadas con el ejercicio de derechos ARCO.	Jefe Nacional de Inteligencia de Negocios

9. DIAGRAMA DE FLUJO



Revisión	Fecha	Autor	Descripción
00	15/09/2023	SGSI	Primera versión
02	09/06/2026	Implementador PDP	Actualización