REGISTRO OFICIAL®
ÓRGANO DE LA REPÚBLICA DEL ECUADOR

SUMARIO:

Págs.

Año I - Nº 163 - 43 páginas
Quito, jueves 13 de noviembre de 2025

Resolución Nro. INEN-INEN-2025-0031-RES

Quito, D.M., 21 de octubre de 2025

SERVICIO ECUATORIANO DE NORMALIZACIÓN

DIRECTOR EJECUTIVO

CONSIDERANDO:

Que, la Constitución de la República del Ecuador publicada en el Registro Oficial 449, del 20 de octubre de 2008 en su artículo 52 dispone que: "*Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características. La ley establecerá los mecanismos de control de calidad y los procedimientos de defensa de las consumidoras y consumidores; y las sanciones por vulneración de estos derechos, la reparación e indemnización por deficiencias, daños o mala calidad de bienes y servicios, y por la interrupción de los servicios públicos que no fuera ocasionada por caso fortuito o fuerza mayor*";

Que, el artículo 226 de la Carta Magna, establece: "*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*";

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

Que, el artículo 320 de la Carta política establece que: "*La producción, en cualquiera de sus formas, se sujetará a principios y normas de calidad, sostenibilidad, productividad sistémica, valoración del trabajo y eficiencia económica y social"*;

Que, el artículo 1 de la Ley del Sistema Ecuatoriano de la Calidad tiene como objetivo establecer el marco jurídico del sistema ecuatoriano de la calidad, destinado a: "*i) regular los principios, políticas y entidades relacionados con las actividades vinculadas con la evaluación de la conformidad, que facilite el cumplimiento de los compromisos internacionales en ésta materia ii) garantizar el cumplimiento de los derechos ciudadanos relacionados con la seguridad, la protección de la vida y la salud humana, animal y vegetal, la preservación del medio ambiente, la protección del consumidor contra prácticas engañosas y la corrección y sanción de estas prácticas y, iii) promover e*

incentivar la cultura de la calidad y el mejoramiento de la competitividad en la sociedad ecuatoriana";

Que, la Ley del Sistema Ecuatoriano de la Calidad publicada en el Suplemento del Registro Oficial No. 26 del 22 de febrero de 2007, en su artículo 3 dispone: "*Declárase política de Estado la demostración y la promoción de la calidad, en los ámbitos público y privado, como un factor fundamental y prioritario de la productividad, competitividad y del desarrollo nacional*";

Que, el Servicio Ecuatoriano de Normalización-INEN, es una entidad técnica de derecho público adscrita al Ministerio de Industrias y Productividad ahora Ministerio de Producción Comercio Exterior, Inversiones y Pesca de conformidad al Decreto Ejecutivo No. 559 de 14 de noviembre de 2018 publicado en el Registro Oficial Suplemento 387 de 13 de diciembre de 2018, fundada el 28 de agosto de 1970, como Instituto Ecuatoriano de Normalización, organismo responsable de promover programas orientados al mejoramiento de la calidad; mediante Decreto Ejecutivo No. 338 dictado el 16 de mayo de 2014 y publicado en el Registro Oficial No. 263 Suplemento, 9 de junio de 2014, en cuyo artículo 2, establece: "*Sustitúyanse las denominaciones del "Instituto Ecuatoriano de Normalización"*, por "Servicio Ecuatoriano de Normalización...";

Que, el artículo 15 de la Ley del Sistema Ecuatoriano de la Calidad, atribuye al Servicio Ecuatoriano de Normalización las siguientes funciones a) "*cumplir las funciones de organismo técnico nacional competente, en materia de reglamentación, normalización y metrología, establecidos en las leyes de la República y en tratados, acuerdos y convenios internacionales, b) Formular, en sus áreas de competencia, luego de los análisis técnicos respectivos, las propuestas de norma, reglamentos técnicos y procedimientos de evaluación de la conformidad, los planes de trabajo, así como las propuestas de las normas y procedimientos metrológicos, g) Previa acreditación, certificación y/o designación, actuar como organismo de evaluación de la conformidad competente a nivel nacional*";

Que, el Reglamento General a la Ley del Sistema Ecuatoriano de la Calidad, en su artículo 30 estipula: "*Para el normal cumplimiento de sus funciones, el INEN elaborará y aplicará los instructivos de funcionamiento necesarios*";

Que, el artículo 32 ibídem establece: "*Para el estudio, formulación y expedición de normas, reglamentos técnicos, procedimientos de evaluación de la conformidad y procedimientos metrológicos, el INEN elaborará la normativa pertinente, misma que se ajustará a recomendaciones y orientaciones internacionales*";

Que, el Reglamento General a la Ley del Sistema Ecuatoriano de la Calidad, en su artículo 36 establece: "*Los servicios técnicos que prestará el INEN al sector público y privado, en función de su infraestructura y recursos estará enmarcado, en los siguientes*

campos: capacitación, calibraciones, ensayos, inspección, certificación, verificación e información técnica, entre otros";

Que, el artículo 47 del Código Orgánico Administrativo, establece: "*La máxima autoridad administrativa de la correspondiente entidad pública ejerce su representación para intervenir en todos los actos, contratos y relaciones jurídicas sujetas a su competencia. Esta autoridad no requiere delegación o autorización alguna de un órgano o entidad superior, salvo en los casos expresamente previstos en la ley*";

Que, el Código Orgánico Administrativo en su artículo 135 señala: "*Le corresponde a la Administración Pública, la dirección del procedimiento administrativo en ejercicio de las competencias que se le atribuyan en el ordenamiento jurídico y en este Código*";

Que, el Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva en su artículo 9 señala: *"(...) Las entidades de la Administración Institucional de la Función Ejecutiva gozan de personalidad jurídica propia para el ejercicio de sus competencias*";

Que, mediante Resolución No. MRL-20120566, de 6 de septiembre de 2012 la Viceministra del Servicio Público del Ministerio de Relaciones Laborales, revisa el cambio de denominación del puesto de Director General a Director Ejecutivo;

Que, mediante Resolución Administrativa No. INEN-INEN-2025-0014-RES de 17 de julio de 2025, suscrito por el Director Ejecutivo del INEN, de ese entonces, publicado en el Suplemento No. 94 del Registro Oficial el 01 de agosto de 2025, se expidio el "*PROCEDIMIENTO PARA LA EMISIÓN DEL CERTIFICADO DE GESTIÓN DE CALIDAD PARA MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS, ARTESANOS CALIFICADOS, PRODUCTORES INDIVIDUALES Y ORGANIZACIONES DE LA ECONOMÍA POPULAR Y SOLIDARIA "MI PRIMER CERTIFICADO INEN*";

Que, mediante Acuerdo Ministerial Nro. MPCEIP-MPCEIP-2025-0037-A, de fecha 30 de julio de 2025 y Acción de Personal Nro. DTH-106 de 31 de julio de 2025, el ministerio de Comercio Exterior, Inversiones y Pesca, encargó a la Mgs. Elizabeth del Roció Guerra Fajardo la Dirección Ejecutiva del Servicio Ecuatoriano de Normalización INEN;

Que, mediante Memorando Nro. INEN-DVC-2025-0423-ME de 16 de septiembre de 2025, la Dirección Técnica de Validación y Certificación, solicita a la Dirección Ejecutiva la modificatoria de los artículos 9 y 12 de la Resolución Administrativa No. INEN-INEN-2025-0014-RES de 17 de julio de 2025, publicado en el Suplemento No. 94 del Registro Oficial el 01 de agosto de 2025, la cual a través del Informe Técnico manifiesta que: "*Con el objetivo de optimizar aspectos puntuales del proceso, sin alterar la estructura fundamental ni comprometer el cumplimiento de los requisitos establecidos en la certificación, asegurando una mayor claridad en la interpretación del*

procedimiento y un compromiso de las organizaciones con la calidad y mejora continua, es necesario la modificatoria(…)";

Que, de conformidad con lo señalado en el artículo 8, numeral 3 del Estatuto por Procesos del Servicio Ecuatoriano de Normalización, es responsabilidad del director ejecutivo, "*Aprobar los instructivos internos y los procedimientos de gestión para la buena marcha de la entidad*";

Que, el numeral 10 del literal b del subnumeral 1.1 del artículo 8 del Estatuto por Procesos del Servicio Ecuatoriano de Normalización en relación al director ejecutivo, establece: "*Suscribir los documentos oficiales, actos y contratos que sean necesarios para el funcionamiento del INEN; pudiendo delegar esta atribución a otros funcionarios, de conformidad con la normativa vigente*";

En uso de las atribuciones y competencias que le confiere el ordenamiento jurídico del país, la Ley del Sistema Ecuatoriano de la Calidad y el Estatuto de Gestión Organizacional por Procesos del Servicio Ecuatoriano de Normalización, INEN

RESUELVE:

Art. 1.- Refórmese el tercer párrafo del artículo 9 de la Resolución Administrativa No. INEN-INEN-2025-0014-RES de 17 de julio de 2025, del Procedimiento para la emisión del Certificado de Gestión de Calidad para Micro, Pequeñas y Medianas Empresas, Artesanos Calificados, Productores Individuales y Organizaciones de la Economía Popular y Solidaria "Mi Primer Certificado INEN", quedando de la siguiente manera:

"Si la organización no remite la documentación requerida y/o no atiende la evaluación en la fecha y hora acordada, se notificará por escrito este particular al solicitante a fin de que, en un término máximo de 30 días contados a partir de la notificación del INEN, se realice la evaluación. Si el solicitante no atiende la evaluación en el término establecido se procederá a cerrar el proceso, notificando formalmente este particular al solicitante y se facturará por el proceso realizado".

Art. 2.- Refórmese el tercer párrafo del artículo 12 de la Resolución descrita, quedando de la siguiente manera:

Para obtener la renovación, la organización deberá cumplir las siguientes condiciones:

- No recibir una calificación de cero (0) en ninguno de los requisitos evaluados".

Art. 3.- De la ejecución de la presente resolución encárguese al/la director/a Técnico/a de Validación y Certificación.

DISPOSICIÓN FINAL

La presente resolución entrará en vigencia a partir de su publicación en el Registro Oficial.

Documento firmado electrónicamente

Mgs. Elizabeth del Rocio Guerra Fajardo
DIRECTORA EJECUTIVA (E)

Referencias:
- INEN-DVC-2025-0423-ME

Anexos:
- informe_para_modificatoria_resolución-2025_mpci-signed0337047001758296779.pdf

Copia:
Señorita Abogada
Johanna Pamela Lopez Benavides
Analista de Asesoria Juridica 1

Señora Magíster
Maritza Natali Taco Tixe
Directora de Asesoria Juridica

mt/ao/ha

Firmado electrónicamente por:
ELIZABETH DEL ROCIO GUERRA FAJARDO
Validar únicamente con FirmaEC

SUPERINTENDENCIA DE BANCOS

RESOLUCIÓN No. SB-DTL-2025-2471

ESTEBAN ANDRÉS FUERTES TERÁN
DIRECTOR DE TRÁMITES LEGALES

CONSIDERANDO:

QUE, el numeral 24 del artículo 62 del Código Orgánico Monetario y Financiero, establece dentro de las funciones otorgadas a la Superintendencia de Bancos, la calificación de los peritos valuadores;

QUE, el artículo 4 del capítulo IV "Normas para la calificación y registro de peritos valuadores", del título XVII "De las calificaciones otorgadas por la Superintendencia de Bancos", del libro I "Normas de control para las entidades de los sectores financieros público y privado", de la Codificación de las Normas de la Superintendencia de Bancos, establece los requisitos para la calificación de los peritos valuadores;

QUE, el artículo 7 del capítulo IV "Normas para la calificación y registro de peritos valuadores", de la norma ibidem establece que la Superintendencia de Bancos dejará sin efecto la resolución de calificación en el evento de que no se actualice la información mencionada en el plazo establecido;

QUE, el inciso quinto del artículo 6 del citado capítulo IV, establece que la resolución de la calificación tendrá una vigencia de diez (10) años contados desde la fecha de emisión de la resolución;

QUE, mediante comunicación ingresada electrónicamente en el Sistema de Calificaciones con hoja de ruta No. SB-SG-2025-43118-E, el Ingeniero Agropecuario Cristhian Andrés Jaramillo Quingla, con cédula No. 1725541450, solicitó la calificación como perito valuador en el área de bienes agropecuarios, entendiéndose que la documentación remitida a la Superintendencia de Bancos es de responsabilidad exclusiva de la parte interesada, que es auténtica y no carece de alteración o invalidez alguna;

QUE, mediante Memorando No. SB-DTL-2025-1145-M de 15 de octubre del 2025, se ha determinado el cumplimiento de lo dispuesto en la norma citada;

QUE, el "Estatuto Orgánico de Gestión Organizacional por Procesos de la Superintendencia de Bancos", expedido con resolución No. SB-2017-893 de 16 de octubre de 2017, dispone como atribución y responsabilidad de la Dirección de Trámites Legales "*e) Calificar a las personas naturales y jurídicas que requieran acreditación de la Superintendencia de Bancos*"; y,

QUE, mediante acción de personal Nro. 0184 de 04 de abril de 2025, fui nombrado Director de Trámites Legales, lo cual me faculta para la suscripción del presente documento,

EN ejercicio de las atribuciones delegadas por el señor Superintendente de Bancos,

RESUELVE:

ARTÍCULO 1.- CALIFICAR al Ingeniero Agropecuario Cristhian Andrés Jaramillo Quingla, con cédula No. 1725541450, como perito valuador en el área de bienes agropecuarios en las entidades sujetas al control de la Superintendencia de Bancos.

ARTÍCULO 2.- VIGENCIA: la presente resolución tendrá vigencia de diez (10) años, contados desde la fecha de emisión, otorgándole el número de registro No. PVQ-2025-02675.

ARTÍCULO 3.- COMUNICAR a la Superintendencia de Compañías, Valores y Seguros con la presente resolución.

ARTÍCULO 4.- NOTIFICAR la presente resolución al correo electrónico cristhianflash@hotmail.com, señalado para el efecto.

COMUNÍQUESE Y PUBLÍQUESE EN EL REGISTRO OFICIAL.- Dada en la Superintendencia de Bancos, en Quito, Distrito Metropolitano, el quince de octubre del dos mil veinticinco.

Mgt. Esteban Andrés Fuertes Terán
DIRECTOR DE TRÁMITES LEGALES

LO CERTIFICO. - Quito, Distrito Metropolitano, el quince de octubre del dos mil veinticinco.

Mgt. Delia María Peñafiel Guzmán
SECRETARIO GENERAL

SUPERINTENDENCIA DE BANCOS
CERTIFICO QUE ES FIEL COPIA DEL ORIGINAL

Firmado electrónicamente por:
DELIA MARIA PENAFIEL GUZMAN
Validar únicamente con FirmaEC

Mgt. Delia María Peñafiel Guzmán
24-10-2025

RESOLUCIÓN No. SCE-DS-2025-68

Mgtr. Hans W. Ehmig Dillon
SUPERINTENDENTE DE COMPETENCIA ECONÓMICA

CONSIDERANDO:

Que el artículo 226 de la Constitución de la República del Ecuador, dispone: *"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 de los derechos reconocidos en la Constitución"*;

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

Que el artículo 233 de la Constitución de la República del Ecuador, dispone: *"Ninguna servidora ni servidor público estará exento de responsabilidades por los actos realizados en el ejercicio de sus funciones o por omisiones, y serán responsables administrativa, civil y penalmente por el manejo y administración de fondos, bienes o recursos públicos* (…)*"*;

Que el objeto del Código Orgánico Administrativo, de conformidad con lo previsto en su artículo 1, es regular el ejercicio de la función administrativa de los organismos que conforman el sector público;

Que el artículo 68 del Código Orgánico Administrativo, establece: *"La competencia es irrenunciable y se ejerce por los órganos o entidades señalados en el ordenamiento jurídico, salvo los casos de delegación, avocación, suplencia, subrogación, descentralización y desconcentración cuando se efectúen en los términos previstos en la ley."*;

Que el número 1 del artículo 69 del Código Orgánico Administrativo, dispone: *"Los órganos administrativos pueden delegar el ejercicio de sus competencias, incluida la de gestión, en: 1. Otros órganos o entidades de la misma administración pública, jerárquicamente dependientes.* (…)*"*;

Que la Superintendencia de Control del Poder de Mercado, fue creada mediante la Ley Orgánica de Regulación y Control del Poder de Mercado, publicada en el Registro Oficial Suplemento Nro. 555, de 13 octubre de 2011, como un órgano técnico de control, con

capacidad sancionatoria, de administración desconcentrada, con personalidad jurídica, patrimonio propio y autonomía administrativa, presupuestaria y organizativa;

Que mediante la *"Ley Orgánica Reformatoria de diversos cuerpos legales, para el fortalecimiento, protección, impulso y promoción de las organizaciones de la economía popular y solidaria, artesanos, pequeños productores, microempresas y emprendimientos"*, publicada en el Suplemento del Registro Oficial Nro. 311, de 16 de mayo de 2023, en su Disposición Reformatoria Segunda, se sustituyó en la Ley Orgánica de Regulación y Control del Poder de Mercado, la frase: *"Superintendencia de Control del Poder de Mercado"* por: *"Superintendencia de Competencia Económica"*; y, *"Superintendente de Control del Poder de Mercado"* por: *"Superintendente de Competencia Económica"*;

Que el artículo 44 de la Ley Orgánica de Regulación y Control del Poder de Mercado, señala: *"Son atribuciones y deberes del Superintendente, además de los determinados en esta Ley:* (…) *11. Dirigir y supervisar la gestión administrativa, de recursos humanos, presupuestaria y financiera de la Superintendencia.* (…)*"*;

Que la Norma 200-05 de las *"Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos"*, en su parte pertinente, establece: *"*(…) *La delegación de competencias debe conllevar, no sólo la exigencia de la responsabilidad por el cumplimiento de los procesos y actividades correspondientes, sino también la asignación de la autoridad necesaria, a fin de que los servidores puedan emprender las acciones más oportunas para ejecutar su cometido de manera expedita y eficaz."*;

Que la Subsecretaría de Contabilidad Gubernamental del Ministerio de Finanzas emitió el *"Instructivo para la Desconcentración de Clases de Registros Contables (Fase 4) Baja y Compensación"*;

Que el 3 de septiembre de 2024, la Asamblea Nacional de conformidad con lo dispuesto en la Constitución de la República del Ecuador y de acuerdo con la Resolución Nro. CPCCS-PLE-SG-040-E-2024-0348, de 15 de agosto de 2024, posesionó al magister Hans W. Ehmig Dillon como Superintendente de Competencia Económica;

Que mediante Resolución Nro. SCE-DS-2025-55, de 29 de agosto de 2025, se resolvió delegar las atribuciones de la máxima autoridad de la Superintendencia de Competencia Económica;

Que mediante memorando Nro. SCE-2025-205, de 20 de octubre de 2025, el Superintendente de Competencia Económica dispuso al Intendente Nacional Jurídico: *"*(…) *la elaboración de una resolución reformatoria a la Resolución Nro. SCE-DS-2025-55, de 29 de agosto de 2025, en la que se incorpore una delegación al Intendente Nacional Administrativo Financiero o a quien haga sus veces en caso de encargo o subrogación, la responsabilidad de aprobar y/o autorizar y disponer la apertura,*

registro, baja, compensación y cierre de cuentas contables observando la normativa legal vigente."; y,

Que es necesario delegar las atribuciones de la máxima autoridad respecto a la gestión de las cuentas por cobrar de la Superintendencia de Competencia Económica, de conformidad con lo que establece el Código Orgánico de Planificación y Finanzas; las Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que Dispongan de Recursos Público, y demás directrices emitidas por el ente rector de las finanzas públicas.

En ejercicio de las atribuciones que le confiere la Ley,

RESUELVE:

REFORMAR LA RESOLUCIÓN Nro. SCE-DS-2025-55, DE 29 DE AGOSTO DE 2025, CON LA CUAL SE RESOLVIÓ DELEGAR LAS ATRIBUCIONES DE LA MÁXIMA AUTORIDAD DE LA SUPERINTENDENCIA DE COMPETENCIA ECONÓMICA

Artículo 1.- Elimínese la letra *"y,"* que consta la final de la letra s) del artículo 5, que contiene la delegación al Intendente Nacional Administrativo Financiero, o a quien cumpla sus funciones en caso de encargo o subrogación.

Artículo 2.- Sustitúyase el texto de la letra t) del artículo 5, que contiene la delegación al Intendente General Administrativo Financiero, o a quien cumpla sus funciones en caso de encargo o subrogación, por el siguiente:

> *"t) Aprobar y/o autorizar y disponer la apertura, registro, baja, compensación y cierre de cuentas contables de conformidad con las disposiciones del Código Orgánico de Planificación y Finanzas Públicas, la Normativa Técnica del Sistema Nacional de Finanzas Públicas, los instructivos y directrices emitidos por el Ministerio de Economía y Finanzas, para lo cual deberá contar con los informes y la documentación necesaria así como también deberá comunicar y/o reportar a los órganos rectores y de control correspondientes de conformidad con normativa vigente; y,"*

Artículo 3.- Incorpórese a continuación de la letra t) del artículo 5, que contiene la delegación al Intendente General Administrativo Financiero, o a quien cumpla sus funciones en caso de encargo o subrogación, lo siguiente:

> *"u) Las demás que el/la Superintendente disponga expresamente en casos particulares por otros medios, siempre y cuando no se contrapongan con las atribuciones estatutarias de los órganos administrativos de la SCE y/o delegaciones realizadas por la Máxima Autoridad."*

DISPOSICIONES GENERALES

PRIMERA.- El Intendente Nacional Administrativo Financiero, o quien cumpla sus funciones en caso de encargo o subrogación, para el cumplimiento de la delegación constante en esta Resolución deberá observar y cumplir la normativa legal vigente aplicable; así como las Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos; directrices y/o normas que emita el Ministerio de Finanzas; normativa institucional y las recomendaciones de Contraloría General del Estado de ser el caso.

SEGUNDA.- Encárguese a la Secretaría General de la publicación y difusión de la presente Resolución en la intranet y en la página web institucional, así como de las gestiones correspondientes para su Publicación en el Registro Oficial de ser el caso.

La presente Resolución entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

CÚMPLASE Y PUBLÍQUESE.-

Dada en la ciudad de Quito, Distrito Metropolitano, el 21 de octubre de 2025.

Firmado electrónicamente por:
HANS WILLI EHMIG DILLON
Validar únicamente con FirmaEC

Mgtr. Hans W. Ehmig Dillon
SUPERINTENDENTE DE COMPETENCIA ECONÓMICA

	FIRMAS DE RESPONSABILIDAD	
Revisado por:	Nombre: Santiago Silva Cargo: **Asesor Despacho**	Firmado electrónicamente por: SANTIAGO DANIEL SILVA ENCALADA Validar únicamente con FirmaEC
	Nombre: Patricio Rubio Román Cargo: **Intendente Nacional Jurídico**	Firmado electrónicamente por: PATRICIO HERNAN RUBIO ROMAN Validar únicamente con FirmaEC
	Nombre: Lorena Caizaluisa Garcés Cargo: **Directora Nacional de Normativa y Asesoría Jurídica**	Firmado electrónicamente por: LORENA ELIZABETH CAIZALUISA GARCES Validar únicamente con FirmaEC
Elaborado por:	Nombre: Isabel Chicaiza Velasteguí Cargo: **Analista 2 de Normativa y Asesoría Jurídica.**	Firmado electrónicamente por: ISABEL LORENA CHICAIZA VELASTEGUI Validar únicamente con FirmaEC

Superintendencia de Protección de Datos Personales

RESOLUCIÓN Nº SPDP-SPD-2025-0040-R

EL SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES

CONSIDERANDO:

Que el numeral 19 del artículo 66 de la Constitución de la República del Ecuador ("CRE") les reconoce y garantiza a las personas 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"*;

Que el artículo 213 de la CRE establece que *"[l]as superintendencias son organismos técnicos de vigilancia, auditoría, intervención y control de las actividades económicas, sociales y ambientales, y de los servicios que prestan las entidades públicas y privadas, con el propósito de que estas actividades y servicios se sujeten al ordenamiento jurídico y atiendan al interés general (...)";* que forman parte de la Función de Transparencia y Control Social; y que, conforme lo dispone el artículo 204 idem, detentan *"personalidad jurídica y autonomía administrativa, financiera, presupuestaria y organizativa (...)"*;

Que a través de la LOPDP se creó la Superintendencia de Protección de Datos Personales ("SPDP") como un órgano de control, con potestad sancionatoria, de administración desconcentrada, con personalidad jurídica y autonomía administrativa, técnica, operativa y financiera, cuyo máximo titular es, de acuerdo con el inciso primero del artículo 76 ídem, el Superintendente de Protección de Datos Personales;

Que el artículo 76 de la LOPDP establece que *"[l]a Autoridad de Protección de Datos Personales es el órgano de control y vigilancia encargado de garantizar a todos los ciudadanos la protección de sus datos personales, y de realizar todas las acciones necesarias para que se respeten los principios, derechos, garantías y procedimientos previstos en la* [Ley Orgánica de Protección de Datos Personales]";

Que el numeral 5 de ese mismo artículo 76 de la LOPDP le confiere a la SPDP funciones, atribuciones y facultades para *"[e]mitir normativa general o técnica, criterios y demás actos que sean necesarios para el ejercicio de sus competencias y la garantía del ejercicio del derecho a la protección de datos personales"*;

Que el primer inciso del artículo 39 de la LOPDP establece que la protección de datos desde el diseño se entiende *"(...) como el deber del responsable del tratamiento de tener en cuenta, en las primeras fases de concepción y diseño del proyecto, que determinados tipos de tratamientos de datos personales entrañan una serie de riesgos para los derechos de los titulares en atención al estado de la técnica, naturaleza y fines del tratamiento, para lo cual, implementará las medidas técnicas, organizativas y de cualquier otra índole, con miras a garantizar el cumplimiento de las obligaciones en materia de protección de datos, en los términos del reglamento"*;

Que el segundo inciso de ese mismo artículo 39 conceptúa a la protección de datos por defecto como aquel deber que tiene el responsable de *"(...) aplicar las medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines del tratamiento, en los términos del reglamento"*;

Que el primer inciso del artículo 59 del Reglamento General de la Ley Orgánica de Protección de Datos Personales ("RGLOPDP") estatuye que *"[e]l responsable del tratamiento tiene la obligación de establecer medidas técnicas y organizativas adecuadas para aplicar los principios establecidos en la normativa de forma eficaz, y proteger los derechos de los titulares, de manera previa al tratamiento de datos personales"*;

Que el segundo inciso del citado artículo 59 del RGLOPDP dispone que, para la fijación de las medidas antedichas, habrán de tomarse en cuenta *"1. La naturaleza, ámbito y finalidad del tratamiento; 2. Los riesgos de diversa probabilidad y gravedad asociados al tratamiento; 3. El estado de la técnica; y, 4. El coste de aplicación"*;

Que el numeral 7 del artículo 80 del RGLOPDP le confiere a la SPDP, además de las atribuciones establecidas en la LOPDP, la de *"[e]mitir guías de referencias que ayuden a los responsables y encargados del tratamiento de datos en el proceso de adecuación y cumplimiento de la normativa de protección de datos personales"*;

Que el artículo 135 del Código Orgánico Administrativo ("COA") determina que *"[l]e corresponde a la Administración Pública, la dirección del procedimiento administrativo en ejercicio de las competencias que se le atribuyan en el ordenamiento jurídico y en este Código (...)"*;

Que mediante resolución N° SPDP-SPDP-2024-0001-R del 2 de agosto del 2024, publicada en el Tercer Suplemento del Registro Oficial N° 624 del 19 de agosto del 2024, el Superintendente de Protección de Datos Personales aprobó el Estatuto Orgánico de Gestión Organizacional por Procesos de Arranque de la Superintendencia de Protección de Datos Personales, reformada mediante resolución N° SPDP-IRD-2025-0028-R, a su vez expedida el 30 de julio del 2025 y publicada en el Registro Oficial N° 105 del 19 de agosto del 2025;

Que la letra b), numeral 2 del artículo 10 de la resolución N° SPDP-SPDP-2024-0001-R establece que a la Intendencia General de Regulación de Protección de Datos Personales ("IRD") le corresponde, entre otras atribuciones y responsabilidades, *"[d]irigir y proponer la elaboración de las propuestas o proyectos normativos para crear, reformar o derogar los actos normativos, sean estos políticas, directrices, reglamentos, resoluciones, lineamientos, normas técnicas, oficios circulares, etcétera, necesarios para el ejercicio de todas las competencias y atribuciones propias de la Superintendencia de Protección de Datos Personales, con los previos informes técnicos de las unidades administrativas sustantivas y adjetivas relacionadas con el ámbito de aplicación de tales normas; así como, todos aquellos actos normativos relacionados con el ejercicio, tutela y procedimientos administrativos de gestión que garanticen a las personas naturales la plena vigencia de sus derechos y deberes previstos en dicha ley y su reglamento (...)"*;

Que la letra c), numeral 2 del artículo 10 de la resolución N° SPDP-SPDP-2024-0001-R, establece, entre las atribuciones y responsabilidades de la IRD, la de *"[d]irigir y proponer la presentación al Superintendente de Protección de Datos Personales de las propuestas de normas, reglamentos, directrices, resoluciones, normas técnicas, oficios circulares, etcétera, vinculados con la regulación de protección de datos personales, para su expedición (...)"*;

Que a través de la letra a) del artículo 4 de la resolución N° SPDP-SPD-2025-0001-R del 31 de enero del 2025, publicada en el Registro Oficial N° 750 del 24 de febrero del 2025, mediante la cual se expidieron las disposiciones, delegaciones de facultades y atribuciones a las autoridades, funcionarios y servidores públicos de la SPDP, se le delegó al Intendente General Regulación de Protección de Datos Personales, entre otras, la responsabilidad de *"[e]mitir normativa general o técnica, criterios y demás actos que sean necesarios para el ejercicio de sus competencias y la garantía del ejercicio del derecho a la protección de datos personales (...)"*;

Que la disposición transitoria del Reglamento para la Elaboración y Aprobación del Plan Regulatorio Institucional de la SPDP —expedido mediante resolución Nº SPDP-SPDP-2024-0018-R del 30 de octubre del 2024, publicada en el Segundo Suplemento del Registro Oficial Nº 679 del 8 de noviembre del 2024— establece que *"(...) el PRI correspondiente a los años fiscales 2024 y 2025 no seguirá el procedimiento establecido en este reglamento y, por ende, se elaborará únicamente a base de los informes técnicos emitidos por las Unidades Administrativas correspondientes; validados por la* [IRD]*; aprobados por el Superintendente o*

su delegado; y, finalmente, publicado en los portales oficiales de la SPDP cuando estén habilitados";

Que mediante la resolución N° SPDP-SPD-2025-0002-R del 3 de febrero del 2025 se aprobó el Plan Regulatorio Institucional del año 2025, dentro del cual se ha establecido la necesidad de expedir los criterios, lineamientos y estándares técnicos, así como los de índole jurídico, sobre la protección de datos personales desde el diseño y por defecto;

Que la IRD, a través del memorando **N° SPDP-IRD-2025-0026-M** suscrito el **28** de **febrero** del **2025,** solicitó a la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales ("IIT") que, en cumplimiento de la resolución N° SPDP-SPD-2025-0002-R por la que se aprueba el Plan Regulatorio Institucional del año 2025, remita el proyecto normativo denominado **Guía de Protección de Datos Personales desde el Diseño y por Defecto;**

Que la IIT, mediante informe técnico **N° INF-SPDP-IIT-2025-0012** del **29** de **julio** del **2025,** se justificó la pertinencia y necesidad de establecer *"(...) una arquitectura de Cero Confianza (Zero Trust) para el tratamiento de datos personales, en tres ejes: Operaciones de desarrollo de privacidad (DevPrivOps), operaciones de desarrollo en seguridad (DevSecOps, y operaciones de desarrollo en riesgos (DevRiskOps) (...)"*;

Que la IIT, mediante memorando **N° SPDP-IIT-2025-0086-M** suscrito el **29** de **julio** del **2025,** la IIT puso en conocimiento de la IRD tanto la **Guía de Protección de Datos Personales desde el Diseño y por Defecto,** como el informe técnico **N° INF-SPDP-IIT-2025-0012,** para cumplir con la resolución N° SPDP-SPD-2025-0002-R que aprueba el Plan Regulatorio Institucional del año 2025;

Que la IRD, mediante informe técnico **Nº INF-SPDP-IRD-2025-0053** del **31** de **julio** del **2025,** justificó la pertinencia y la necesidad de establecer obligaciones y lineamientos en protección de datos desde el diseño y por defecto, alineados con la gestión de riesgos para la adecuada aplicación por parte de los responsables del tratamiento, por lo que, en su parte pertinente, expone: *"(...) [l]a SPDP en ejercicio de sus funciones y atribuciones está facultada de conformidad con el numeral 5 del artículo 76 de la LOPDP para emitir (...) la Guía de Protección de Datos Desde el Diseño y por Defecto (...)"; y, recomendó: "(...) iniciar con el proceso de socialización en cumplimiento con lo dispuesto por la Resolución N° SPDP-SPDP-2024-0022-R para que en el término de veinte (20) días la ciudadanía pueda realizar sus aportes"*;

Que mediante memorando **N° SPDP-IRD-2025-0144-M** suscrito el **31** de **julio** del **2025,** la IRD puso en conocimiento de la Dirección de Asesoría Jurídica ("DAJ") el proyecto normativo denominado **Guía de Protección de Datos Personales desde el Diseño y por Defecto,** así como el informe técnico **N° INF-SPDP-IRD-2025-0052,** para que en el término de diez (10) días se pronuncie sobre la concordancia con la normativa y la legalidad, de conformidad con lo dispuesto en la resolución N° SPDP-SPDP-2025-0022-R;

Que la DAJ, mediante informe **N° INF-SPDP-DAJ-2025-0032** del **31** de **julio** del **2025,** en su parte pertinente, determinó que la **Guía de Protección de Datos Personales desde el Diseño y por Defecto** es congruente con los principios establecidos en la LOPDP, no transgrede o contradice normas matrices, cumple con el principio de legalidad y, por ende, recomendó que *"(...) [l]a IRD debe solicitar a quien corresponda la publicación a través de la página web institucional e informar su publicación a través de las redes sociales institucionales, con la finalidad de que la ciudadanía, las organizaciones de la sociedad civil o interesados en general, de manera motivada, puedan remitir sus observaciones o realizar aportes respecto del contenido (...)"*;

Que mediante memorando **N° SPDP-DAJ-2025-0067-M** suscrito el **31** de **julio** del **2025,** la DAJ puso en conocimiento de la IRD el informe técnico **N° INF-SPDP-DAJ-2025-0032,** así

como la validación legal del proyecto normativo que contiene la **Guía de Protección de Datos Personales desde el Diseño y por Defecto;**

Que mediante memorando **N° SPDP-IRD-2025-0145-M** suscrito el **31** de **julio** del **2025,** la IRD solicitó a las unidades administrativas de la SPDP que procedan con las acciones pertinentes a fin de que publiquen, en la página web institucional y redes sociales de la SPDP, el borrador de la **Guía de Protección de Datos Personales desde el Diseño y por Defecto,** para que el proyecto normativo esté disponible para la ciudadanía, las organizaciones de la sociedad civil y los demás interesados desde el 1 de agosto hasta el 1 de septiembre del 2025, inclusive, con el objeto de poder recibir sus observaciones o aportes, siempre que estuvieren debidamente motivados;

Que en cumplimiento de la resolución N° SPDP-SPDP-2024-0022-R, se ejecutó el proceso de socialización de la **Guía de Protección de Datos Personales desde el Diseño y por Defecto** dentro del término de veinte (20) días, de conformidad con el artículo 12 de la misma resolución;

Que a través de informe técnico **N° INF-SPDP-IRD-2025-0088,** suscrito el **15** de **octubre** del **2025,** la IRD incorporó, al informe técnico, las observaciones y los aportes que se consideraron relevantes y adecuados, previa justificación de las modificaciones realizadas al proyecto normativo;

Que mediante memorando **N° SPDP-IRD-2025-0200-M** suscrito el **15** de **octubre** del **2025,** la IRD remitió todo el expediente al suscrito Superintendente de Protección de Datos Personales para que realice en observaciones correspondientes o, en su caso, para que lo apruebe;

En Ejercicio de sus atribuciones constitucionales, legales y reglamentarias,

Resuelve:

Art. 1.- Aprobar la ***Guía de Protección de Datos Personales desde el Diseño y por Defecto*** ("la Guía"), cuya autoría corresponde a los señores Luis Enríquez Álvarez, Intendente General de Innovación Tecnológica y Seguridad de Datos Personales, y Daniel Hernández Ortiz, Especialista de Innovación Tecnológica y Seguridad de Datos Personales, en concordancia con lo establecido en los artículos 39 y 40 de la LOPDP, el artículo 59 del RGLOPDP, así como con el literal b), numeral 2, del artículo 10 de la resolución N° SPDP-SPDP-2024-0001-R; todo ello con el objetivo de precautelar la adecuada implementación de las medidas de seguridad de naturaleza técnica y organizativa.

Art. 2.- Establecer que los principios desarrollados en los capítulos 1 y 2 de la Guía serán de cumplimiento obligatorio, siempre que resulten aplicables de acuerdo con la naturaleza, el alcance y las características de un específico contexto de tratamiento de datos personales.

En lo demás, el contenido de la Guía tendrá un carácter orientativo. Su aplicación, en todo caso, se la tendrá como una *buena práctica* y *recomendación técnica* para fortalecer la gestión de riesgos y la adecuación progresiva hacia el principio de protección de datos personales desde el diseño y por defecto.

Disposición General

En el plazo de un (1) año contado partir de la publicación de esta resolución en el Registro Oficial, la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales:

a. Ejecutará la revisión y evaluación del contenido de la Guía, con el objeto de procurar la mejora continua de dicho instrumento; y,

b. Hecho lo anterior, presentará el informe técnico pertinente que deberá poner en conocimiento del Superintendente de Protección de Datos Personales.

Disposición Transitoria

Sin perjuicio de la vigencia de esta resolución —y de conformidad con la resolución Nº SPDP-SPDP-2024-0018-R y con la resolución Nº SPDP-SPDP-2024-0022-R—, la SPDP emitirá la normativa técnica que considere necesaria en materia de protección de datos personales desde el diseño y por defecto, para precautelar el tratamiento adecuado de los derechos y libertades fundamentales de los titulares.

DISPOSICIÓN FINAL

Esta resolución entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Dada y firmada en Quito, D. M., el 21 de octubre del 2025.

Firmado electrónicamente por:
FABRIZIO ROBERTO PERALTA DIAZ
Validar únicamente con FirmaEC

FABRIZIO PERALTA-DÍAZ
SUPERINTENDENTE DE PROTECCIÓN DE DATOS PERSONALES


spdp
Guía
de Protección de Datos Personales
desde el Diseño y por Defecto
Superintendencia de Protección de Datos Personales
Intendencia General de Innovación Tecnológica
y Seguridad de Datos Personales
2025

GUÍA DE PROTECCIÓN DE DATOS PERSONALES DESDE EL DISEÑO Y POR DEFECTO

INTRODUCCIÓN

La Ley Orgánica de Protección de Datos Personales (LOPDP) regula la protección de datos personales desde el diseño y por defecto como un principio que establece obligaciones para los responsables del tratamiento de datos personales, que es aplicable durante las fases de concepción y diseño de un proyecto. Estas obligaciones se fundamentan en la adecuada gestión de los riesgos en el tratamiento de datos personales en el futuro.

La Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales, expedida el 29 de abril del 2025 y publicada en el Cuarto Suplemento del Registro Oficial N° 41 del 19 de mayo del 2025, regula los principios fundamentales de la gestión de riesgos para la protección de los derechos y las libertades de los titulares de los datos, define las cinco etapas necesarias para la gestión del riesgo, así como la evaluación de impacto en el tratamiento de datos personales.

La Superintendencia de Protección de Datos Personales, en ejercicio de sus competencias administrativas, publica en esta oportunidad la **Guía de Protección de Datos Personales desde el Diseño y por Defecto,** que tiene como fin determinar, de forma específica, la gestión de riesgos en las etapas de diseño y de ejecución de un proyecto que involucre el tratamiento de datos personales. No obstante, este documento también será útil para quienes ya tengan implementados procesos que involucren el tratamiento de datos personales y requieran una transformación de conformidad con la LOPDP, su Reglamento General y la normativa secundaria emitida por la Superintendencia de Protección de Datos Personales.

Esta guía ha sido desarrollada por Luis Enríquez Álvarez (Intendente General de Innovación Tecnológica y Seguridad de Datos Personales) y por Daniel Hernández Ortiz (Especialista de Innovación Tecnológica y Seguridad de Datos Personales). El documento fue editado por Vanessa Hervás Novoa, asesora de Despacho.

Quito, D. M., octubre 21 del 2025.

Fabrizio Peralta-Díaz
Superintendente de Protección de Datos Personales

Tabla de contenido

0. Definiciones y abreviaciones

Array. Conjunto de elementos o datos almacenados en ubicaciones contiguas de la memoria.

DAST. Análisis dinámico de seguridad de aplicaciones.

DevOps. Operaciones de desarrollo de *software*.

DevPrivOps. Desarrollo de operaciones en privacidad.

DevSecOps. Desarrollo de operaciones en seguridad de la información.

DevRiskOps. Desarrollo de operaciones en gestión de riesgos.

EDS. Espacio de *sampleo*.

EGS. Evaluación global de procesos.

IaC. Escaneo de infraestructura como código.

LOPDP. Ley Orgánica de Protección de Datos Personales.

Pipelines CI/CD. Flujo de integración y despliegue continuo con validaciones.

PET. Tecnologías de mejoramiento de la privacidad.

RAT. Registro de Actividades del Tratamiento.

Rationale. Justificación de las métricas, modelos de riesgo y criterios utilizados para calibrar los componentes del riesgo.

RLOPDP: Reglamento General de la Ley Orgánica de Protección de Datos Personales.

ROSI. Retorno a la inversión en seguridad.

SAST. Análisis estático de seguridad de aplicaciones.

SCA. Análisis de la composición del *software*.

Shift Left. Principios para la integración temprana de la seguridad.

1. Contexto de la obligación

Esta guía tiene carácter orientativo. Los principios establecidos en los capítulos 1 y 2 son de obligatorio cumplimiento, siempre y cuando sean aplicables y necesarios en un contexto de desarrollo, personalización e implementación de un *software* y/o sistemas de información que involucren el tratamiento de datos personales. Por otro lado, el capítulo 2 proporciona algunas tácticas recomendadas que podrán ser escogidas de manera proporcional al riesgo, tamaño, complejidad y contexto de la actividad de tratamiento de datos personales. El capítulo 3 es optativo pero recomendado. Este documento es concordante con la **Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales**.

El artículo 39 de la Ley Orgánica de Protección de Datos Personales (LOPDP) establece: *"(...) Se entiende a la protección de datos desde el diseño como el deber del responsable del tratamiento de tener en cuenta, en las primeras fases de concepción y diseño del proyecto, que determinados tipos de tratamientos de datos personales entrañan una serie de riesgos para los derechos de los titulares en atención al estado de la técnica, naturaleza y fines del tratamiento, para lo cual, implementará las medidas técnicas, organizativas y de cualquier otra índole, con miras a garantizar el cumplimiento de las obligaciones en materia de protección de datos, en los términos del reglamento"*[1]. En toda actividad de desarrollo, personalización o implementación de un *software* y/o sistemas de información que realicen un tratamiento de datos personales, el responsable del tratamiento deberá cumplir con lo establecido en el principio de protección de datos personales desde el diseño y por defecto. No obstante, para los casos de obligaciones de conformidades específicas, se procederá de acuerdo con lo establecido en el artículo 11 de la LOPDP.

La implementación del principio de protección de datos desde el diseño y por defecto puede ser descompuesta de la siguiente manera:

1.1. Protección de datos desde el diseño

Implica considerar dentro de la planificación de un proyecto que involucre el tratamiento de datos personales, los riesgos que éste podría ocasionar a los derechos y libertades de los titulares de los datos, es decir, la protección de datos desde el diseño está enfocada en los riesgos futuros que el tratamiento puede ocasionar. En este sentido, las medidas de seguridad que se planifiquen deben alinearse en un contexto multidimensional del riesgo, involucrando principalmente riesgos jurídicos y riesgos operacionales.

1.2. Protección de datos por defecto

El término 'por defecto' debe entenderse como los valores preexistentes o preseleccionados en las opciones de configuración que, se implementen para el tratamiento de datos personales. La configuración 'por defecto' se aplicará sin menoscabar obligaciones legales. Desde la perspectiva del responsable del tratamiento, es necesario configurar de manera preestablecida el principio de pertinencia y minimización de datos, así como los mecanismos para el ejercicio de los derechos de los titulares de datos; entre ellos, el derecho de acceso,

[1] Ley Orgánica de Protección de Datos Personales (LOPDP), art. 39.

el derecho de eliminación, el derecho a la portabilidad de datos y los demás establecidos en la LOPDP.

2. Arquitectura de Cero Confianza en el tratamiento de datos personales (*Zero Trust Data Protection*)

El diseño de una arquitectura de **Cero Confianza** para el tratamiento de datos personales es una macroestrategia que, consiste en no otorgar confianza implícita a cualquier operación o táctica que involucre el tratamiento de datos personales. La arquitectura de **Cero Confianza** procede del ámbito de la seguridad de la información[2], pero su utilidad estratégica es óptima y adaptable al ámbito de la protección de datos personales. Implica principios generales que deben ser implementados en las operaciones de desarrollo de *software* (*DevOps*) y en la planificación e implementación de operaciones que involucren el tratamiento de datos personales.

Considerando que los riesgos de protección de datos son multidimensionales, es fundamental integrar principios para el desarrollo e implementación de sistemas que realicen un tratamiento de datos personales en tres dimensiones: desarrollo de operaciones en privacidad (*DevPrivOps*), desarrollo de operaciones en seguridad de la información (*DevSecOps*) y desarrollo de operaciones en gestión de riesgos (*DevRiskOps*). Varios de los principios fundamentales en estas tres dimensiones de la protección de datos personales son explicados a continuación. No obstante, los responsables del tratamiento podrán agregar e implementar los que consideren necesarios, de acuerdo con las condiciones particulares del tratamiento de datos personales que realicen.

2.1. Desarrollo de operaciones en privacidad

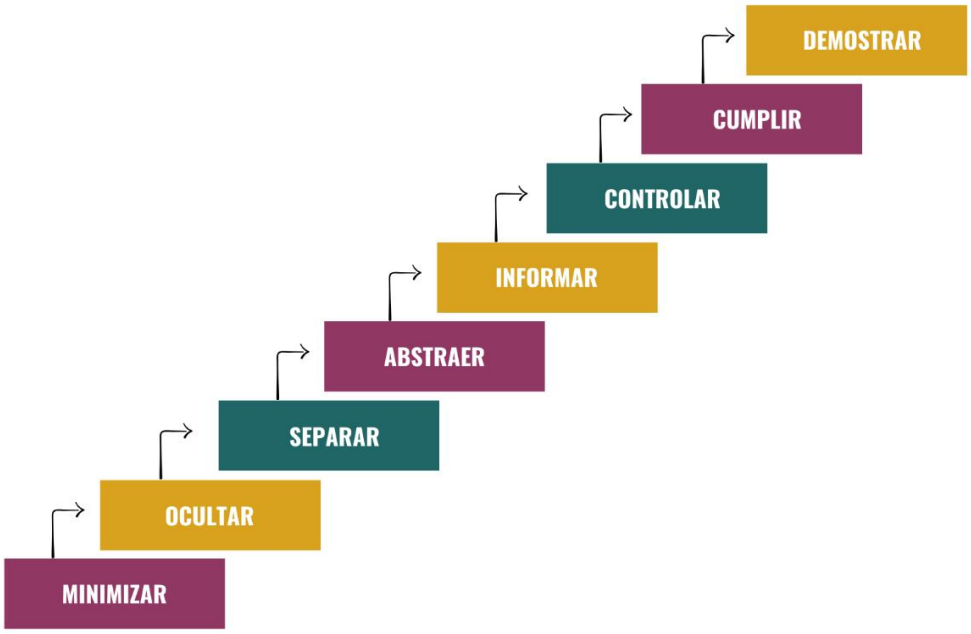


Figura 1: Principios para el desarrollo de operaciones en privacidad

[2] Ver, Rose S., Borchet O., *et al.*, Zero Trust Architecture, NIST Special Publication 800-207, Estados Unidos, 2020.

Los siguientes ocho principios para el desarrollo de operaciones en privacidad, han sido considerados como fundamentales, tanto por autores relevantes[3] como por otras autoridades de protección de datos[4]. La finalidad de estos principios es hacer que el principio de protección de datos desde el diseño y por defecto sea implementado en todo tratamiento de datos personales.

2.1.1. Minimizar. Consiste en usar la menor cantidad de datos personales posible para cumplir con los fines necesarios del tratamiento. Las estrategias y operaciones de minimización de datos necesitan una gestión de riesgos que permitan identificar con claridad, cuáles son los datos realmente necesarios para cumplir una finalidad. Esto se debe a que todo tratamiento de datos implica riesgos; y, en consecuencia, un valor al riesgo[5].

Tácticas. Es recomendable implementar las siguientes tácticas:

- ✓ Seleccionar. Solicitar únicamente datos y atributos relevantes de personas naturales. No recolectar datos personales irrelevantes.

- ✓ Excluir. Excluir datos y atributos irrelevantes de personas naturales, es decir, todo lo que no ayude a cumplir con los fines lícitos y legítimos del tratamiento.

- ✓ Remover. Remover datos en cuanto ya no sean necesarios para cumplir con los fines estrictamente necesarios del tratamiento.

- ✓ Eliminar. Destruir y borrar datos personales, incluyendo los de las copias de respaldo (*backups*), siempre y cuando sea técnicamente posible.

2.1.2. Ocultar. Esta estrategia consiste en desvincular los atributos de la identidad de los titulares de los datos personales.

Tácticas. A nivel táctico pueden utilizarse mecanismos para restringir, ofuscar, disociar y evitar correlaciones entre los datos personales que potencialmente puedan llegar a identificar a una persona natural.

- ✓ Restringir. Implementar controles de acceso a datos personales de naturaleza organizacionales y técnicos que impidan el acceso a personas no autorizadas.

- ✓ Ofuscar. Prevenir la legibilidad de los datos personales con técnicas de mejoramiento de la privacidad, tales como: esteganografía, *data masking*, cifrado columnar y otros métodos de privacidad diferencial.

- ✓ Disociar. Romper los vínculos entre personas naturales, eventos y datos.

- ✓ Mezclar. Mezclar datos personales para ocultar los atributos de la identidad.

[3] Ver, Hoepman J., *Privacy Design Strategies (The Little Blue Book)*, Radboud University, Países Bajos, 2018-2022.
[4] Ver, AGENCIA ESPAÑOLA DE PROTECCION DE DATOS, Guía de Privacidad desde el Diseño, AEPD, 2019.
[5] Ver, Enríquez L., *A Personal Data Value at Risk (Pd-VaR) Approach*, Journal or Research Innovation and Technologies, RITHA Publishing, 2024.

2.1.3. Separar. Consiste en separar los tratamientos de datos que pueden identificar, de manera directa o indirecta, a una persona natural. Para ello, es recomendable utilizar diferentes bases no vinculadas, evitando el almacenamiento centralizado de datos personales. El principio de separación es óptimo para evitar el fácil perfilamiento de los titulares de datos personales. En el contexto de la gestión de bases de datos, se recomienda utilizar medidas de separación, como el eliminar los identificadores específicos de cada tabla o utilizar seudónimos.

Tácticas. Es recomendable implementar las siguientes tácticas:

- ✓ Aislar. Registrar y procesar datos personales en diferentes bases de datos, separadas de manera lógica o física (*hardware*).

- ✓ Distribuir. Repartir el tratamiento de bases de datos personales en diferentes servidores que no estén bajo el control de una misma entidad. Esto incluye el tratamiento de datos en sistemas de arquitectura distribuida.

2.1.4. Abstraer. Consiste en limitar al máximo los detalles de los datos personales objeto de tratamiento. Se distingue de la estrategia de minimización en la medida en que se enfoca en el nivel de detalle con el que son tratados los datos personales. A nivel táctico, abstraer datos personales requiere evaluar el grado de detalles necesarios para identificar a un titular de datos en un determinado contexto. Cabe considerar que atributos como la edad, el género o las preferencias pueden ser suficientes para identificar a una persona natural en determinados espacios de *sampleo*. Es necesario implementar medidas de sumarización, agregación o perturbación que minimicen los detalles de los datos personales tratados. Por ejemplo, agregar ruido en los datos para alterar el dato personal original.

Tácticas. Es recomendable implementar las siguientes tácticas:

- ✓ Sumarizar. Resumir los atributos particulares en atributos más generales.

- ✓ Agrupar. Procesar información acerca de un grupo de personas, en lugar de información de cada persona natural en particular.

- ✓ Perturbar. No exponer el valor real de los datos, sino aproximaciones de ellos, transformaciones algorítmicas o agregar ruido.

2.1.5. Informar. Se fundamenta en el derecho a la información establecido en el artículo 12 de la LOPDP. Consiste en implementar las medidas organizacionales necesarias para facilitar la información a los titulares de los datos, sobre todo aspectos relacionados con el tratamiento de sus datos, así como explicar las razones por las cuales es necesario el tratamiento de datos y notificar a los titulares de acuerdo con lo establecido en la LOPDP.

Tácticas. Es recomendable implementar las siguientes tácticas:

- ✓ Suministrar. Informar con transparencia a los titulares de los datos, todo lo concerniente con el tratamiento de sus datos personales.

- ✓ Explicar. Explicar claramente a los titulares los motivos y las finalidades del tratamiento de sus datos personales.

- ✓ Notificar. Comunicar a los titulares cuando sus datos personales fuesen compartidos a terceros o cuando exista una vulneración a la seguridad, de acuerdo con lo establecido en la LOPDP.

2.1.6. Controlar. Consiste en dar mecanismos a los titulares de los datos para controlar el tratamiento de sus datos personales. A nivel táctico, es necesario implementar mecanismos para que los titulares de los datos puedan otorgar y revocar su consentimiento, escoger medidas alternativas para su consentimiento (como servicios pagados) y ejercer sus derechos establecidos en la LOPDP (como el derecho de rectificación, actualización, portabilidad, eliminación, oposición, suspensión). Por ejemplo, implementar mecanismos que permitan al titular de los datos ejercer estos derechos a través de su sitio *web*; o, al menos, contar con un medio de contacto como correo electrónico o chat que los gestione con celeridad.

Tácticas. Es recomendable implementar las siguientes tácticas:

- ✓ Consentir. Recoger el consentimiento explícito, informado, inequívoco y transparente de los titulares de datos.

- ✓ Escoger. Otorgar a los titulares de datos la posibilidad de otorgar un consentimiento libre que no esté absolutamente condicionado por una relación hegemónica de poder.

- ✓ Actualizar. Proveer a los titulares de los datos, mecanismos para actualizar o solicitar la rectificación de sus datos personales.

- ✓ Retraer. Proveer a los titulares de los datos mecanismos de ejercicio de derechos, tales como de oposición o de suspensión del tratamiento de sus datos personales.

2.1.7. Cumplir. Consiste en cumplir en la práctica con la protección de datos personales. Los principios del tratamiento de datos personales, los derechos de las personas concernidas y toda obligación establecida en la LOPDP debe ser implementada en la práctica y no solo en la teoría. En función de aquello, es necesario desarrollar una política de protección de datos personales que cumpla con el deber ser; pero más importante aún, es implementar en la práctica una gestión de riesgos para la protección de los derechos y libertades mediante controles de riesgos de manera eficaz y eficiente. Para ello, el responsable del tratamiento deberá designar al personal especializado de la institución para la implementación de los controles jurídicos, organizacionales y técnicos. En este sentido, es fundamental contar con una política de protección de datos personales que integre los controles jurídicos, organizacionales y técnicos necesarios, así como monitoree los cambios de circunstancias que puedan suscitarse y así actualizar tanto la política de protección de datos personales como su implementación.

Tácticas. Es recomendable implementar las siguientes tácticas:

- ✓ Responsabilizar. El responsable del tratamiento de datos debe alinear la protección de datos personales a las estrategias y los objetivos de su objeto de negocio. Este compromiso debe plasmarse en políticas institucionales.

- ✓ Mantener. Mantener una declaración de aplicabilidad con la justificación y la descripción de medidas de seguridad jurídicas, organizacionales y técnicas. Implementarlas es una obligación.

- ✓ Monitorear. Auditar la eficacia y eficiencia de los controles de riesgo implementados, pues las circunstancias pueden cambiar en el tiempo.

2.1.8. Demostrar. Consiste en demostrar, en la práctica, que se está cumpliendo con las obligaciones establecidas en la LOPDP. Este principio exige registrar todos los procesos que involucren el tratamiento de datos personales, auditarlos en los ámbitos jurídico, organizacional y técnico; y, elaborar reportes que permitan dar cumplimiento a los controles establecidos por la SPDP.

Tácticas. Es recomendable implementar las siguientes tácticas:

- ✓ Registrar. Documentar los procesos decisionales de la institución y guardar los registros de los tratamientos de datos personales.

- ✓ Auditar. Verificar la actualización, la autenticidad y la integridad de los registros de actividades del tratamiento de datos personales de manera regular y periódica, incluyendo los incidentes de seguridad ocurridos en un lapso determinado.

- ✓ Reportar. Guardar los eventos de manera confidencial y presentarlos a la SPDP cuando estos sean requeridos.

2.2. Desarrollo de operaciones en seguridad de la información

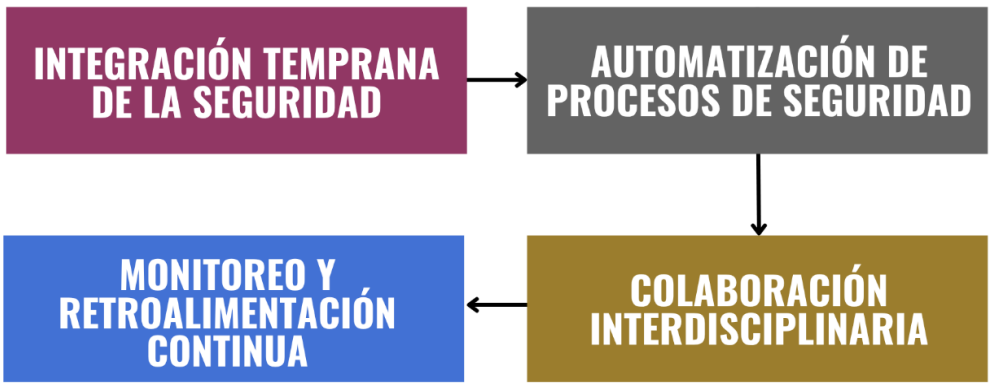


Figura 2: Principios para el desarrollo de operaciones en seguridad

DevSecOps es una evolución de *DevOps* que integra la seguridad en todas las fases del ciclo de vida del desarrollo de *software*, promoviendo una cultura de colaboración entre los equipos de desarrollo, operaciones y seguridad. Su objetivo es garantizar que la seguridad sea una responsabilidad compartida y se aborde desde el inicio del proceso de desarrollo[6]. Cabe especificar que estos principios son obligatorios únicamente cuando haya desarrollo o personalización de *software*.

[6] Para ampliar su conocimiento sobre principios, herramientas y mejores prácticas se recomienda el siguiente artículo. Pynt. "DevSecOps Principles, Tools, and Best Practices [2025 Guide]." *Pynt Learning Hub*. Consultado el 21 de abril de 2025. https://www.pynt.io/learning-hub/devsecops/devsecops-principles-tools-and-best-practices-2025-guide.

A continuación, se establecen cuatro principios estratégicos básicos de *DevSecOps*, pero cada responsable del tratamiento puede agregar otros principios que considere adecuados para sus necesidades específicas:

2.2.1. Integración Temprana de la Seguridad ("*Shift Left*"). Es la implementación de prácticas de seguridad desde las etapas iniciales del desarrollo, como el diseño y la codificación. Al hacerlo, se identifican y corrigen vulnerabilidades de manera más eficiente y económica. En el contexto de la protección de datos personales, esto se traduce en la implementación temprana de controles como el cifrado, la autenticación robusta y la minimización de datos, asegurando que la protección de datos personales esté integrada desde el inicio del desarrollo del proyecto.

2.2.2. Automatización de Procesos de Seguridad. La automatización de controles de seguridad a lo largo del ciclo de desarrollo, integración, prueba y despliegue de aplicaciones es la base del proceso de seguridad. El propósito de la automatización es que cada cambio en el *software* sea verificado en tiempo real contra un conjunto de reglas predefinidas de seguridad.

Esto se implementa mediante herramientas y procesos que incluyen:

a) Análisis estático de seguridad de aplicaciones (*SAST*)[7]. Analiza el código fuente o binario en busca de vulnerabilidades antes de que la aplicación se ejecute; como fugas de datos, mal manejo de excepciones o uso de funciones criptográficas obsoletas.

b) Análisis dinámico de seguridad de aplicaciones (*DAST*)[8]. Prueba la aplicación mientras está en ejecución para detectar vulnerabilidades como inyecciones *SQL*, *XSS*, fallos de autenticación o exposición de datos a través de la interfaz *web*.

c) Análisis de la composición del *software* (SCA)[9]. Detecta componentes de terceros o librerías de *software* vulnerables utilizadas en el proyecto esencial para la verificación de funciones críticas como encriptación o gestión de sesiones.

d) Escaneo de infraestructura como código (IaC)[10]. Automatiza la revisión de archivos de infraestructura como: *Terraform*, *CloudFormation* o *Kubernetes*, para garantizar que los recursos como bases de datos, contenedores de almacenamiento y redes virtuales estén configurados con políticas seguras, sin exposición pública.

e) Detección de fuga de datos[11]. Escaneos automatizados que identifican posibles exposiciones de información sensible como tokens, contraseñas o datos personales directamente en el código o en archivos de configuración.

f) Flujo de integración y despliegue continuo con validaciones[12]. Cada vez que se realiza un cambio, el sistema ejecuta automáticamente todas las pruebas de seguridad previas antes

[7] *Static Application Security Testing*.
[8] *Dynamic Application Security Testing*.
[9] *Software Composition Analysis*.
[10] *Infraestructure as code*.
[11] *Data Leakage Detection*.
[12] *Pipelines CI/CD*.

de permitir el despliegue, evitando que las vulnerabilidades se detecten recién en el ambiente de producción.[13]

La automatización no reemplaza completamente al juicio humano, pero permite que las prácticas de seguridad se integren de forma constante, homogénea y a gran escala.

2.2.3. Colaboración interdisciplinaria. La colaboración entre los equipos de desarrollo, operaciones, seguridad y protección de datos personales constituye un componente esencial en la implementación del enfoque *DevSecOps*. Esta integración garantiza que las decisiones relacionadas con la seguridad se tomen de manera informada y conjunta, reduciendo la fragmentación de responsabilidades y promoviendo la coherencia en la aplicación de controles técnicos. Esta colaboración permite que las políticas de protección de datos personales se traduzcan en medidas técnicas específicas y se apliquen de forma consistente a lo largo de todo el ciclo de desarrollo. El intercambio continuo de información entre disciplinas facilita la identificación oportuna de riesgos asociados al tratamiento de datos sensibles y la implementación de medidas de seguridad preventivas o correctivas[14].

Por ejemplo:

a) Validar desde el diseño que las funcionalidades cumplan con principios de minimización y acceso restringido.

b) Asegurar que los entornos de prueba no expongan datos reales sin las debidas medidas de control de riesgos.

c) Implementar y monitorear controles de acceso y trazabilidad acordes con los niveles de sensibilidad de la información tratada.

2.2.4. Monitoreo y Retroalimentación Continua. El monitoreo continuo en entornos *DevSecOps* constituye un elemento fundamental para la detección oportuna de vulnerabilidades, comportamientos anómalos y accesos no autorizados que puedan comprometer la seguridad de los datos personales. A través de herramientas de observabilidad integradas en las canalizaciones de despliegue continuo, se posibilita una retroalimentación constante que permite ajustar políticas, corregir configuraciones inseguras y fortalecer mecanismos de control de acceso.

Lo descrito se alinea con la necesidad de adoptar un enfoque preventivo y adaptativo frente a la gestión de riesgos asociados al tratamiento de datos personales. En particular, la implementación de entornos con sistemas de detección de intrusos, monitoreo de registros en tiempo real y alertas automatizadas constituye una práctica esencial para mejorar la trazabilidad, la rendición de cuentas y la protección efectiva de la información[15].

[13] Ver Feio C., *et al.*, *An Empirical Study of DevSecOps Focused on Continuous Security Testing*, EuroS&PW 2024.
[14] Ver Abiona O., *et al.*, *The emergence and importance of DevSecOps: Integrating and reviewing security practices within the DevOps pipeline*, *World Journal of Advanced Engineering Technology and Sciences*, 2024.
[15] Prates L. y Pereira R., *DevSecOps practices and tools*. *International Journal of Information Security*, 2024.

2.3. Desarrollo de operaciones en gestión de riesgos

Figura 3: Principios para el desarrollo de operaciones en riesgos.

Dado que la LOPDP se fundamenta en la gestión de riesgos, es importante considerar los principios que fundamentan todos los procedimientos que son empleados tanto en las operaciones *DevPrivOps*, como en las operaciones *DevSecOps*. Estos principios son una adaptación de los principios fundamentales definidos en la **Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales**, pero a nivel macroestratégico, en el contexto de la protección de datos personales desde el diseño y por defecto.

2.3.1. Gestión de riesgos para la protección de derechos y libertades. Este principio consiste en realizar una gestión de riesgos para la protección de derechos y libertades desde la concepción de un proyecto que involucre el tratamiento de datos personales. Gracias a ello, el responsable del tratamiento podrá elaborar y comparar escenarios de riesgos probables contra los derechos y libertades de los titulares de los datos, con el fin de realizar su evaluación de impacto del tratamiento de datos personales. Consecuentemente, es necesario realizar por defecto una gestión de riesgos para la protección de los derechos y libertades futuros con la finalidad de escoger e implementar las operaciones *DevPrivOps* y *DevSecOps* necesarias.

2.3.2. Integración de la gestión de riesgos para la protección de derechos y libertades con la gestión riesgos de seguridad de la información. Este principio consiste en integrar los resultados de la gestión de riesgos para la protección de los derechos y libertades de los titulares de los datos con la gestión de riesgos de seguridad de la información. En el mundo

real, no existe protección de datos sin seguridad de la información, pues ambos tipos de riesgos son interdependientes. En el contexto de la protección de datos desde el diseño y por defecto, se recomienda integrar las operaciones *DevPrivOps* con las *DevSecOps* para mitigar riesgos desde la concepción de un proyecto que involucre el tratamiento de datos personales.

2.3.3. Utilizar estándares de mejores prácticas. Consiste en escoger las mejores guías y estándares para las operaciones *DevPrivOps* y *DevSecOps* que pueden orientar de mejor manera a los responsables del tratamiento de datos. Estas deberán ser complementadas con métricas significativas y modelos de riesgo adecuados que ayuden a reducir la incertidumbre acerca de futuros proyectos que involucren el tratamiento de datos personales.

2.3.4. Justificación de todos los *rationales.* Consiste en justificar todo valor de entrada en un modelo de riesgos como parte de la aplicación del principio de protección de datos desde el diseño y por defecto. En este contexto, se trata de justificar los valores de entrada y criterios utilizados en la implementación de las operaciones *DevPrivOps* y *DevSecOps*. Es fundamental integrar este principio desde la concepción de un proyecto que involucre el tratamiento de datos personales.

2.3.5. Conformidad en riesgos. Consiste en evitar a toda costa una conformidad sólo en el papel; y, más bien, asegurar en la práctica la identificación, análisis y evaluación de riesgos desde la concepción misma de un proyecto que involucre el tratamiento de datos personales. En el contexto de las operaciones *DevPrivOps* y *DevSecOps*, se recomienda aplicarlas en diversos escenarios de riesgo, lo cual ayudará al responsable del tratamiento a seleccionar e implementar las tácticas más adecuadas.

2.3.6. Auditorías. Consiste en auditar las operaciones *DevPrivOps* y *DevSecOps* en función de su eficacia y eficiencia. Para ello, se recomienda auditar la permeabilidad de cada una de las operaciones *DevPrivOps* y *DevSecOps* analizando sus probabilidades reales de cumplimiento y el retorno a la inversión en seguridad (ROSI)[16] eficaz y eficiente que pueden brindar a los responsables del tratamiento de datos.

2.3.7. Prevenir vulneraciones de la seguridad de datos personales. Consiste en enfocarse en la prevención de vulneraciones de la seguridad de datos personales desde la concepción de un proyecto que involucre el tratamiento de datos personales. Es necesario gestionar la efectividad de las operaciones *DevPrivOps* y *DevSecOps* en función de la reducción de la probabilidad de ocurrencia y del impacto de potenciales vulneraciones de la seguridad de datos personales en sus tres dimensiones: confidencialidad, integridad y disponibilidad.

[16] *Return on Security Investment*.

3. Criterios para estimar la madurez de la permeabilidad de los principios de *DevPrivOps, DevSecOps y DevRiskOps*

En el contexto de una arquitectura de **Cero Confianza** en el tratamiento de datos personales, es necesario tener un mecanismo de evaluación. Es recomendable disponer de un modelo que permita evaluar el grado de madurez de un responsable del tratamiento de datos en la adopción y aplicación de estos principios. La permeabilidad de los principios es una misión continua y sucesiva; por la cual, los responsables del tratamiento ganarán la experiencia para futuros proyectos que involucren el tratamiento de datos personales. No obstante, la arquitectura de **Cero Confianza** puede ser utilizada en procesos nuevos o cuando se transforman procesos ya existentes para alcanzar su conformidad a la LOPDP, su Reglamento y la normativa emitida por la Superintendencia de Protección de Datos Personales.

A continuación, se muestra un prototipo de sistema para evaluar el nivel de madurez de un responsable del tratamiento en los principios de **Cero Confianza** en el tratamiento de datos personales. Cabe aclarar que este sistema de estimación de madurez es recomendable, pero no obligatorio, ya que pueden existir otros modelos de evaluación de madurez que se ajusten mejor a las circunstancias específicas de una actividad de tratamiento de datos personales. Asimismo, puede haber actividades de tratamiento de datos personales que no necesariamente requieran la implementación de todas la *DevSecOps*, tal y como constan en el ejemplo, los procesos que no realizan un tratamiento automatizado de datos personales. El siguiente ejemplo de sistema puede ser utilizado tanto para analizar y evaluar cada principio en particular, como para hacer un análisis de cumplimiento de todos los principios en los tres ejes correspondientes a *DevPrivOps, DevSevOps y DevRiskOps*.

3.1. Niveles de madurez

Para analizar el nivel de madurez de cada principio en particular se recomiendan los siguientes niveles:

Nivel de madurez de cada principio por proceso de tratamiento de datos

Nivel 0 – Caótico. El principio no es conocido o no es considerado como necesario por el responsable del tratamiento del proceso que involucra el tratamiento de datos personales. Este equivale a un 0% de madurez.
Nivel 1 – Implícito. El principio es conocido y asumido como necesario, pero ha sido implementado en menos del 25% del proceso que involucra el tratamiento de datos personales.
Nivel 2 – Temprano explícito. El principio es conocido, asumido como necesario y ha sido implementado de manera parcial entre el 25% y el 75% del proceso que involucra el tratamiento de datos personales.
Nivel 3 – Maduro explícito. El principio es conocido, asumido como necesario y ha sido implementado en más del 75 % del proceso que involucra el tratamiento de datos personales.

Tabla 1: Niveles de madurez.

La estimación de cada principio para una actividad de tratamiento de datos personales debe tener un *rationale* cuantitativo o cualitativo, explicados en la **Guía de Gestión de Riesgos**

y Evaluación de Impacto del Tratamiento de Datos Personales. Los resultados de la gestión de riesgos para la protección de los derechos y libertades servirán para calibrar de manera adecuada todos los valores de entrada para establecer el nivel de madurez en la implementación del principio de protección de datos desde el diseño y por defecto, en un lapso determinado.

3.2. Método de calibración

Para poder estimar el nivel de madurez de los principios de *DevPrivOps, DevsevOps y DevRiskOps* es necesario seguir los siguientes pasos:

3.2.1. Identificación. Contar con un registro de actividades del tratamiento (RAT) que permita identificar y clasificar los procesos que involucran el tratamiento de datos personales. Este registro deberá contener de manera granular cada tratamiento de datos personales. No obstante, puede que un principio se haya implementado parcialmente. El total de procesos de tratamiento de datos personales constituye el espacio de *sampleo*.

Por ejemplo:

REGISTRO DE ACTIVIDADES DEL TRATAMIENTO EN UN COLEGIO

ACTIVIDADES DE TRATAMIENTO	TIPOS DE DATOS PERSONALES	RESPONSABLE DEL PROCESO
Registro de matrículas de estudiantes.	Datos de niñas, niños y adolescentes, datos de los padres y madres, datos comportamentales, datos simples de registro.	Secretaría General
Pagos con tarjeta de crédito	Datos financieros	Departamento financiero
Registro de historias médicas	Datos relativos a la salud	Departamento médico
[...]	[...]	[...]

Tabla 2: Ejemplo de registro.

3.2.2. Análisis y evaluación. Consiste en estimar la permeabilidad del principio en cada proceso que involucra el tratamiento de datos personales en base a *rationales* cuantitativos o cualitativos. El principio debe estar respaldado por los correspondientes controles de riesgos que sean eficaces y eficientes. No obstante, puede que un principio se haya implementado parcialmente; para lo cual, se puede utilizar el nivel de madurez pertinente. Se pueden utilizar tablas para el registro de evaluación:

ACTIVIDAD DEL TRATAMIENTO: Registro de matrículas de estudiantes

DevPrivOps

PRINCIPIO DE CERO CONFIANZA	EVALUACIÓN
Minimizar	2
Ocultar	1
Separar	0
Abstraer	0
Informar	3
Controlar	3
Cumplir	3
Demostrar	2

DevSecOps

PRINCIPIO DE CERO CONFIANZA	EVALUACIÓN
Integración temprana	3
Automatización	2
Colaboración interdisciplinaria	3
Monitoreo	1

DevRiskOps

PRINCIPIO DE CERO CONFIANZA	EVALUACIÓN
Gestión de riesgos para protección de derechos y libertades	3
Integración con la gestión de riesgos de seguridad de la información	0
Utilizar estándares de mejores prácticas	3
Justificación de *rationales*	1
Conformidad en riesgos	2
Auditorías	3
Prevenir vulneraciones de seguridad de datos personales	2

Tabla 3: Ejemplo de evaluación de cada principio.

3.3. Evaluación por eje

Una vez que se ha analizado y evaluado el estado de madurez de cada principio por separado, en relación con las actividades de tratamiento de datos personales, el siguiente paso es tener una visión global de todo en conjunto. No obstante, esta evaluación de nivel de madurez se realiza en un plano estratégico, en función de la incorporación y permeabilidad de los principios asociados a los ejes de *DevPrivOps, DevSecOps y DevRiskOps*. Una vez que se haya hecho la selección e implementación de las medidas de seguridad correspondientes, se deberá realizar la gestión del riesgo inherente, en función de la **Guía de Gestión de Riesgos**

y Evaluación de Impacto del Tratamiento de Datos Personales; y, evaluar el estado de madurez del principio de protección de datos desde el diseño y por defecto con los resultados obtenidos.

3.3.1. Nivel de madurez de todos los principios juntos. Es un sistema cualitativo similar al presentado para evaluar la implementación de cada principio en una actividad de tratamiento de datos en particular, pero con el objetivo de analizar de manera correlacionada con todos los procesos que involucren el tratamiento de datos personales. Para ello, se recomienda lo siguiente:

Nivel 0 – Caótico. Los principios no son conocidos o no son considerados como necesarios por el responsable del tratamiento (0%).
Nivel 1 – Implícito. Los principios son conocidos y asumidos como necesarios, pero han sido implementados en menos del 25% de procesos que involucran tratamiento de datos personales.
Nivel 2 – Temprano explícito. Los principios son conocidos y asumidos como necesarios y han sido implementados de manera parcial entre el 25% y el 75% de los procesos que involucran el tratamiento de datos personales.
Nivel 3 – Maduro explícito. Los principios son conocidos y asumidos como necesarios y han sido implementado en más del 75 % de los procesos que involucran el tratamiento de datos personales.

Tabla 4: Nivel de madurez de todos los principios juntos

3.3.2. Calibración de cada eje. Para estimar el nivel de madurez en cada uno de los ejes es necesario considerar tres variables:

a) Espacio de *sampleo* (EDS). El espacio de *sampleo* es igual a todos los procesos que, involucran el tratamiento de datos personales en un eje específico. Consideremos el ejemplo anterior, un colegio es el responsable del tratamiento de datos y tiene diez actividades de tratamiento de datos personales. EDS = 10.

b) Evaluación global de procesos (EGP). Es la calificación global asignada a los procesos que involucran el tratamiento de datos personales en cada uno de los ejes. Del ejemplo anterior, podemos representar cuántos procesos están en nivel caótico, en nivel implícito, en nivel temprano explícito y el nivel maduro explícito. De esta manera, podemos estimar el total de los niveles de un mismo principio en las diez actividades del tratamiento.

Array DevPrivOps = [minimizar, ocultar, separar, abstraer, informar, controlar, cumplir, demostrar]

Array DevSecOps = [integración temprana, automatización de procesos, colaboración multidisciplinaria, monitoreo]

Array DevriskOps = [gestión de riesgos para protección de derechos y libertades, integración con la seguridad de la información, estándares de mejores prácticas, *rationales*, conformidad en riesgos, auditorías, prevención de vulneraciones de seguridad]

Actividad de Tratamiento	***DevPrivOps***	***DevSecOps***	***DevRiskOps***
Tratamiento 1	[2, 1, 0, 0, 3, 3, 3, 2]	[3, 2, 3 ,1]	[3, 0, 3, 1, 0, 2, 2]
Tratamiento 2	[1, 2, 0, 0, 2, 2, 3, 1]	[3, 2, 3, 1]	[3, 0, 3, 2, 0, 1, 3]
Tratamiento 3	[0, 0, 0, 1, 3, 2, 3, 3]	[1, 2, 3, 0]	[2, 1, 3, 2, 1, 1, 2]
Tratamiento 4	[2, 1, 0, 0, 2, 2, 2, 3]	[3, 1, 2, 1]	[2, 2, 2, 1, 2, 2, 2]

Tratamiento 5	[0, 0, 3, 3, 2, 1, 2, 3]	[2, 0, 3, 1]	[2, 1, 3, 2, 0, 2, 3]
Tratamiento 6	[1, 0, 3, 1, 3, 3, 2, 3]	[3, 1, 3, 2]	[3, 1, 3, 0, 1, 2, 1]
Tratamiento 7	[0, 1, 2, 1, 3, 3, 3, 3]	[2, 1, 3, 3]	[1, 1, 3, 3, 2, 3, 2]
Tratamiento 8	[1, 2, 2, 2, 2, 3, 3, 3]	[2, 0, 3, 1]	[2, 1, 3, 2, 1, 0, 3]
Tratamiento 9	[3, 1, 1, 0, 3, 2, 2, 3]	[3, 1, 1, 3]	[3, 0, 2, 3, 2, 3, 2]
Tratamiento 10	[0, 1, 2, 2, 3, 3, 3, 3]	[1, 0, 2, 3]	[3, 2, 3, 2, 2, 2, 3]

Tabla 5: Calibración de cada eje.

Nivel de madurez *DevPrivOps* = [minimizar (1.0), ocultar (0.9), separar (1.3), abstraer (1.0), informar (2.6), controlar (2.4), cumplir (2.6), demostrar (2.7)]

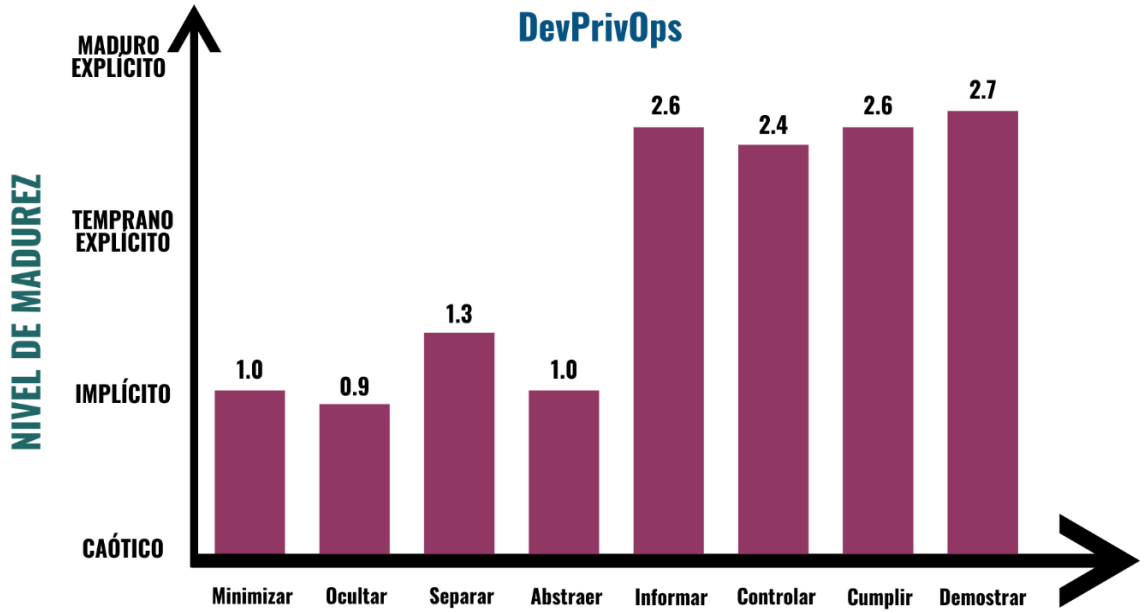


Figura 4: Nivel de madurez *DevPrivOps*

Nivel de madurez *DevSecOps* = [integración temprana (2.3), automatización de procesos (1.0), colaboración multidisciplinaria (2.6), monitoreo (1.6)]

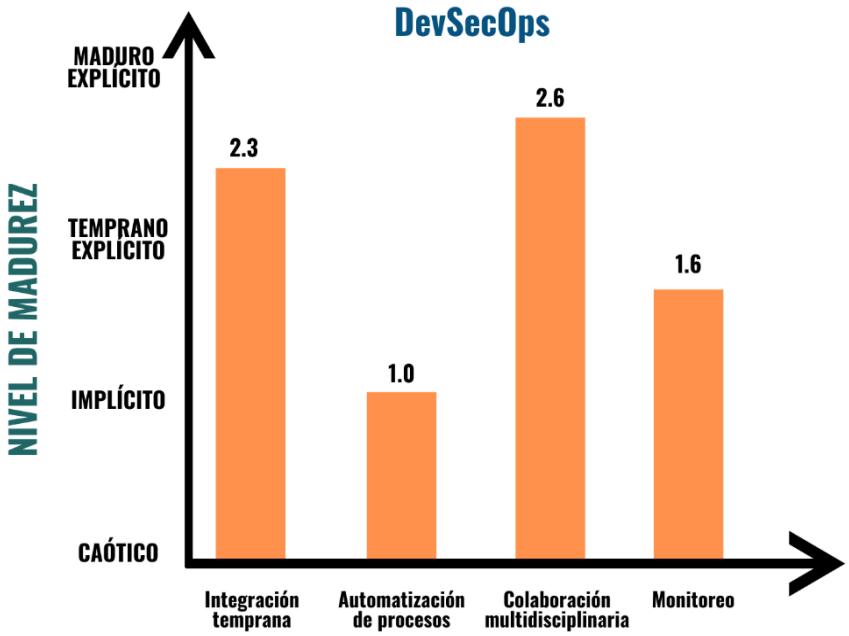


Figura 5: Nivel de madurez *DevSecOps*

Nivel de madurez *DevRiskOps* = [gestión de riesgos para la protección de los derechos y libertades (2.4), integración con la seguridad de la información (0.9), estándares de buenas prácticas (2.8), *rationales* (1.8), conformidad en riesgos (1.1), auditorías (1.8), prevención de vulneraciones (2.3)]

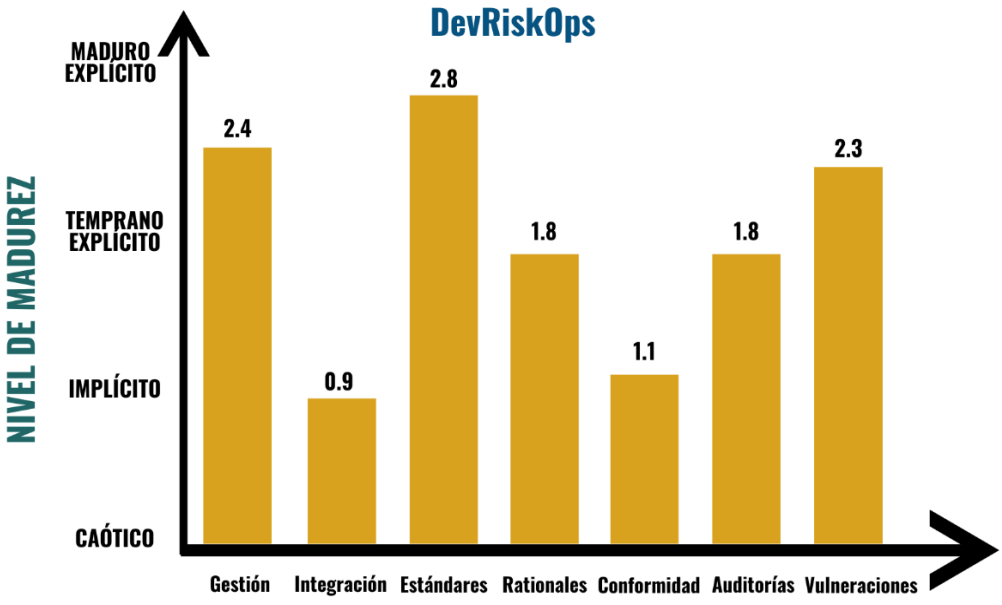


Figura 6: Nivel de madurez *DevRiskOps*

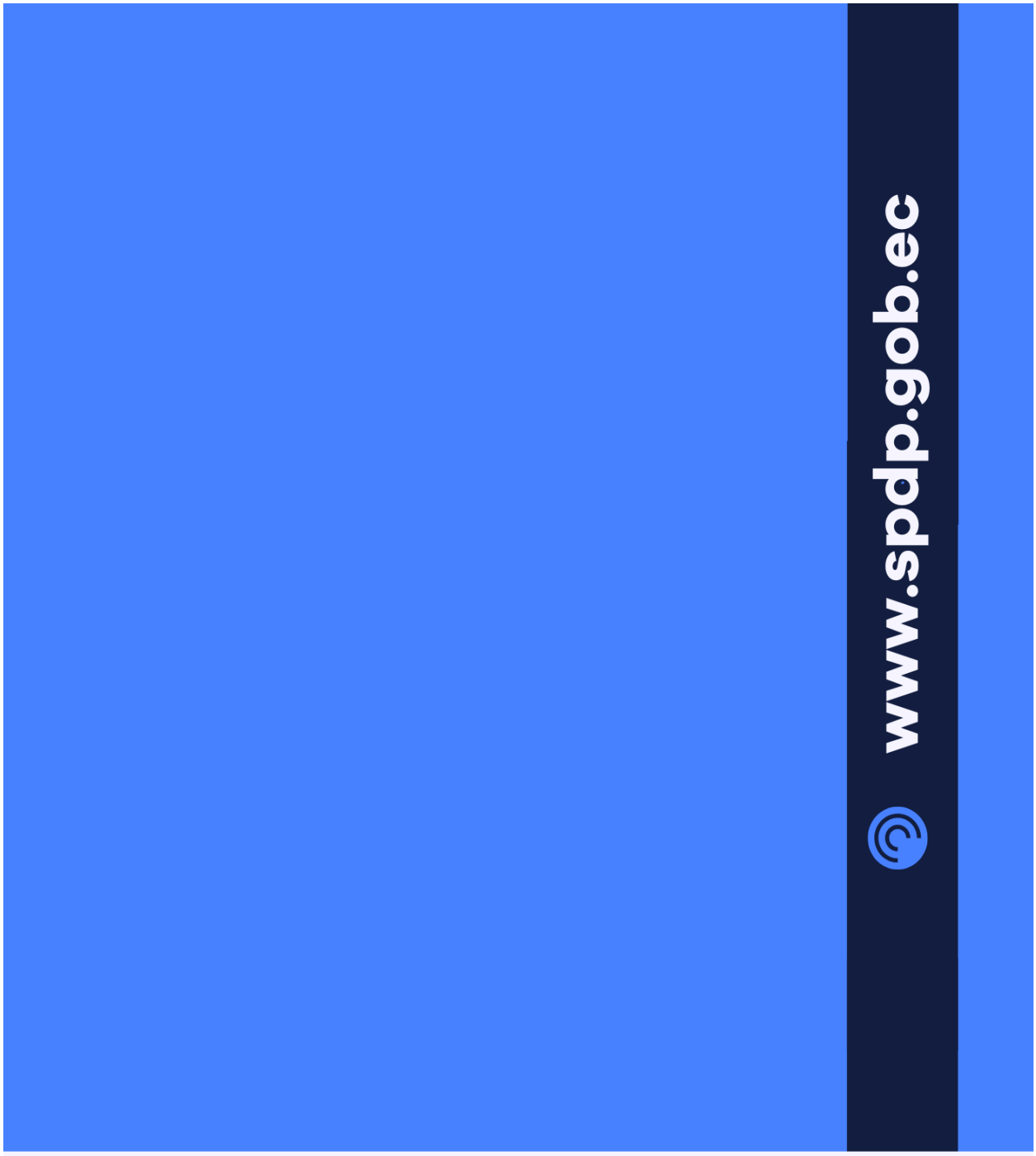
4. Disposiciones transitorias

4.1. Guía complementaria

Esta guía será complementada por una guía de controles de riesgos para la protección de datos personales que, será emitida en un plazo máximo de seis meses de la publicación oficial de este documento. Cubrirá las principales Tecnologías de mejoramiento de la privacidad (*Privacy Enhancing Technologies*) y expondrá de manera práctica la implementación de controles de privacidad diferencial, con especial énfasis en la ciencia de datos y la arquitectura de los sistemas de inteligencia artificial.

4.2. Actualizaciones

Esta guía será actualizada anualmente.


www.spdp.gob.ec
Superintendencia de Protección de Datos Personales
Av. Amazonas y Unión Nacional de Periodistas.
Plataforma Gubernamental de Gestión Financiera.
Bloque Amarillo, piso 5 (externo).
Quito – Ecuador

Mgs. Jaqueline Vargas Camacho
DIRECTORA (E)

Quito:
Calle Mañosca 201 y Av. 10 de Agosto
Atención ciudadana
Telf.: 3941-800
Ext.: 3134

www.registroficial.gob.ec

NGA/FMA

El Pleno de la Corte Constitucional mediante Resolución Administrativa No. 010-AD-CC-2019, resolvió la gratuidad de la publicación virtual del Registro Oficial y sus productos, así como la eliminación de su publicación en sustrato papel, como un derecho de acceso gratuito de la información a la ciudadanía ecuatoriana.

"Al servicio del país desde el 1º de julio de 1895"