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

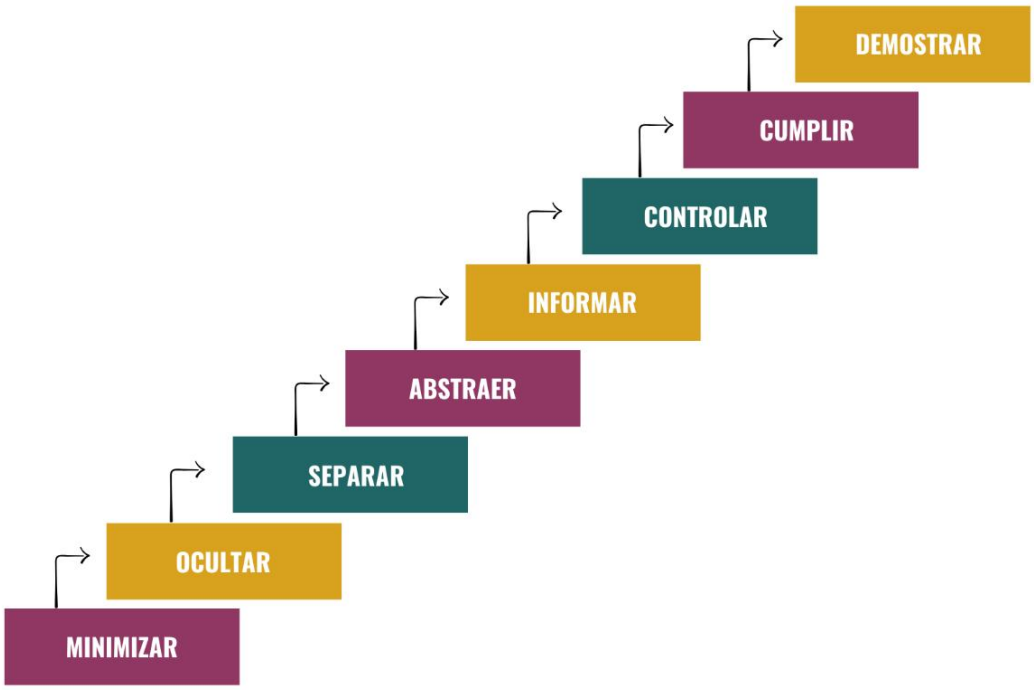

Figura 1: Principios para el desarrollo de operaciones en privacidad

[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

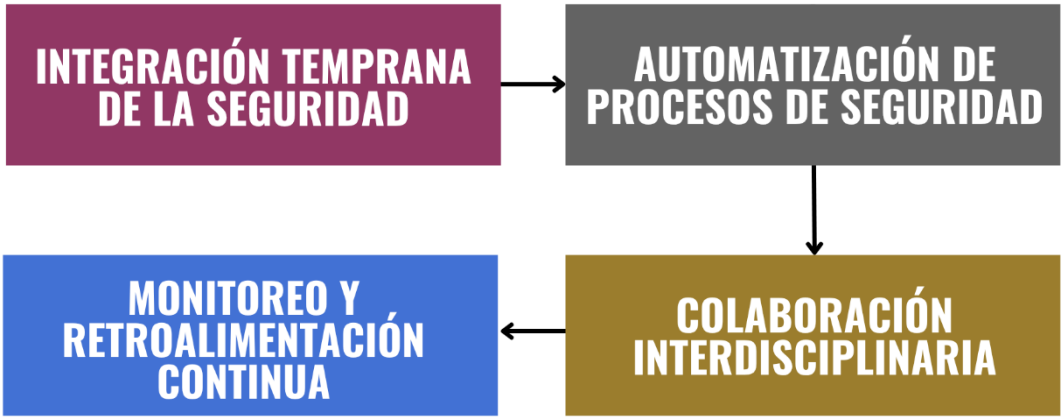

Figura 2: Principios para el desarrollo de operaciones en seguridad

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)]

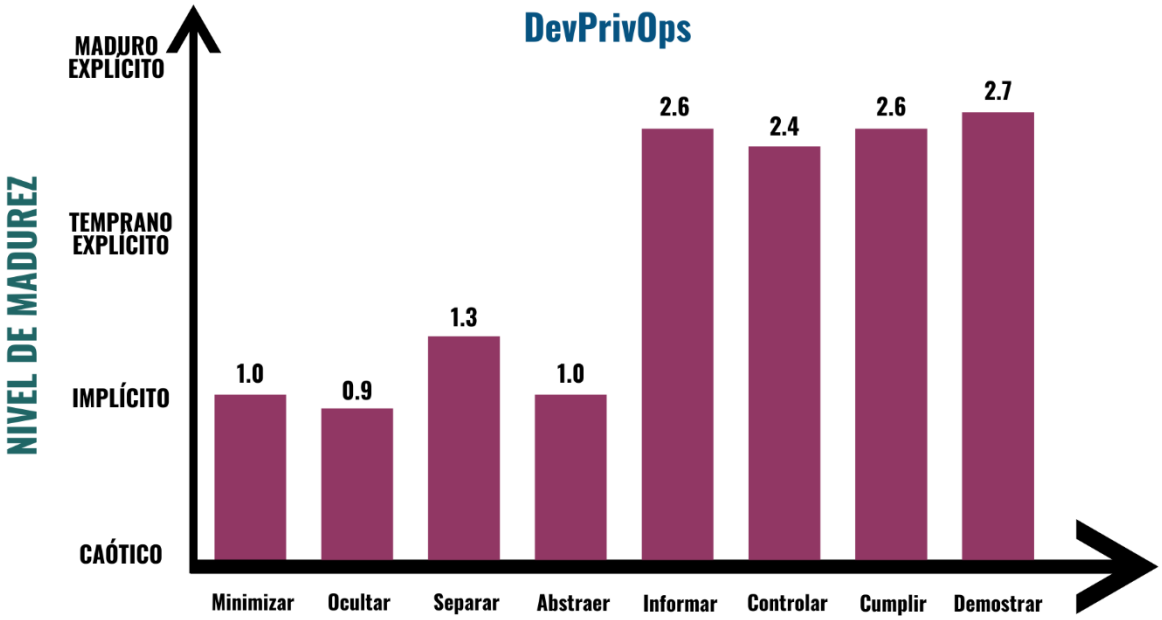

Figura 4: Nivel de madurez *DevPrivOps*

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

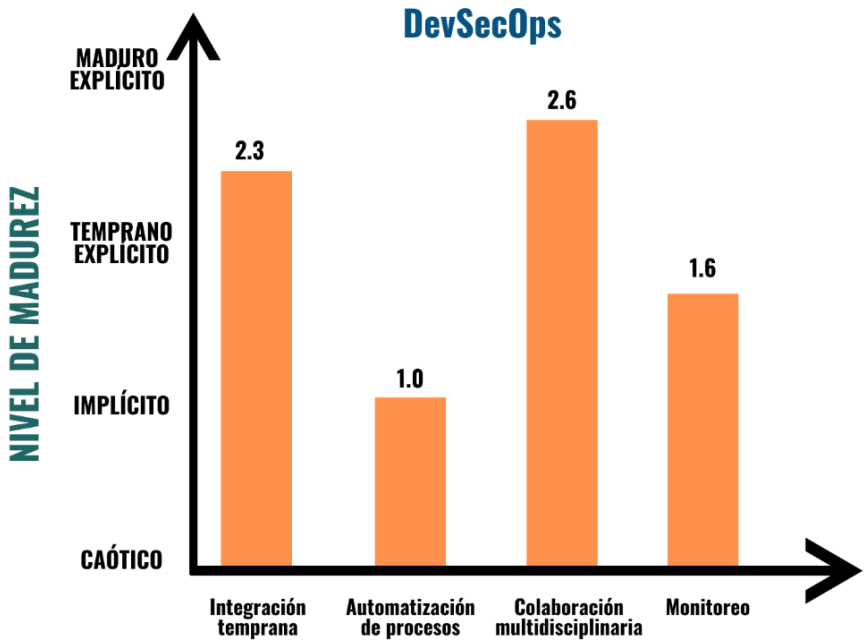

Figura 5: Nivel de madurez *DevSecOps*

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)]

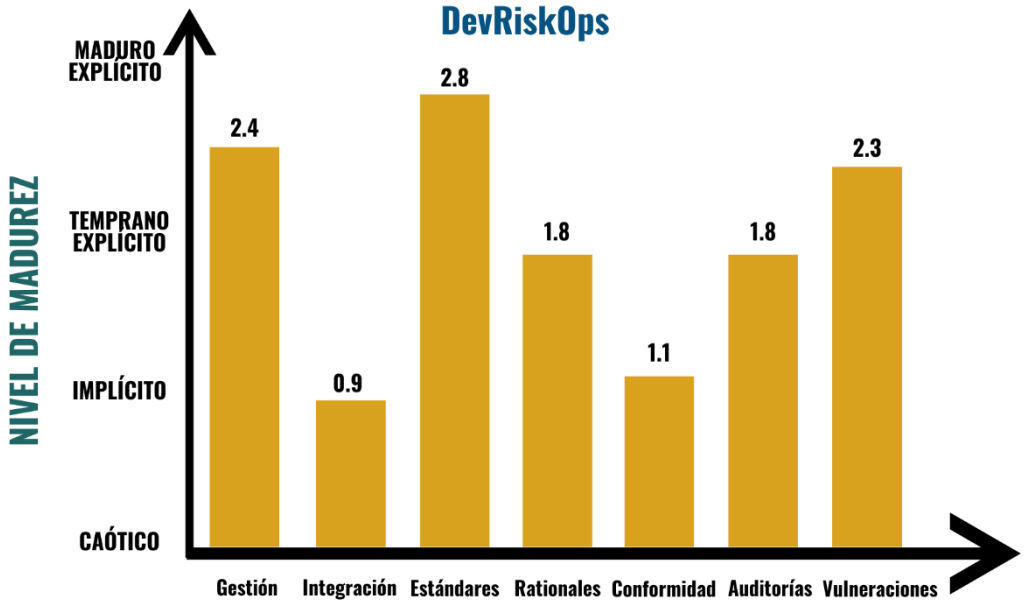

Figura 6: Nivel de madurez *DevRiskOps*

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