SUPERINTENDENCIA DE PROTECCIÓN
DE DATOS PERSONALES

GUÍA DE PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

INTENDENCIA GENERAL DE INNOVACIÓN TECNOLÓGICA Y SEGURIDAD DE DATOS PERSONALES

2025

GUÍA DE PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

INTRODUCCIÓN

La Ley Orgánica de Protección de Datos Personales establece el principio de protección de datos desde el diseño y por defecto en el artículo 39, estableciendo obligaciones para los Responsables del tratamiento de datos personales para las fases de concepción y diseño del proyecto. Estas obligaciones se fundamentan en la gestión de riesgos, pero una gestión de riesgos para el tratamiento de datos personales en el futuro. La *guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales* publicada en marzo de 2025, es una guía extensiva que ya abarca los principios fundamentales de una gestión de riesgos para la protección de derechos y libertades, las cinco etapas necesarias para la gestión del riesgo inherente, y las evaluaciones de impacto del tratamiento de datos personales. Consecuentemente, la presente guía es una extensión que tiene como fin abarcar en específico la gestión de riesgos en las etapas tempranas de un proyecto que involucre el tratamiento de datos personales.

La Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales, dentro del marco de sus competencias, se complace en publicar la presente obra titulada "Guía de Protección de datos desde el diseño y por defecto ". Esta guía ha sido desarrollada de manera general por Luis Enríquez (Intendente General de Innovación Tecnológica y Seguridad de Datos Personales), y por Daniel Hernández (Especialista de Innovación Tecnológica y Seguridad de Datos Personales).

CONTENIDOS

1. Contexto de la obligación

El artículo 39 de la Ley Orgánica de Protección de Datos Personales 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]. La protección de datos por defecto hace referencia a que el responsable debe 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”. La implementación de esta obligación puede ser descompuesta de la siguiente manera:

1.1. Protección de datos desde el diseño

Consiste en considerar, dentro de la planificación de un proyecto que involucre el tratamiento de datos personales, los riesgos que este tratamiento podría ocasionar contra los derechos y libertades de los titulares de datos. Esto quiere decir, que la protección de datos desde el diseño se fundamenta en la gestión de riesgos, pero no del riesgo inherente de un tratamiento de datos, sino más bien, de riesgos futuros que el tratamiento puede ocasionar. 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 un tratamiento de datos personales. Desde la perspectiva del responsable del tratamiento, es necesario configurar de manera preestablecida los principios de protección de personales, como el principio de minimización de datos, el principio de eliminación de datos, o los mecanismos para el ejercicio de los derechos de los titulares de datos, tales como el derecho de acceso, el derecho a la portabilidad de datos, y todos los establecidos en la LOPDP.

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

El diseño de una arquitectura de Cero Confianza para el tratamiento de datos personales es una macro-estrategia que consiste en no otorgar confianza implícita en cualquier operación o táctica que involucre el tratamiento de datos personales. La arquitectura de Cero

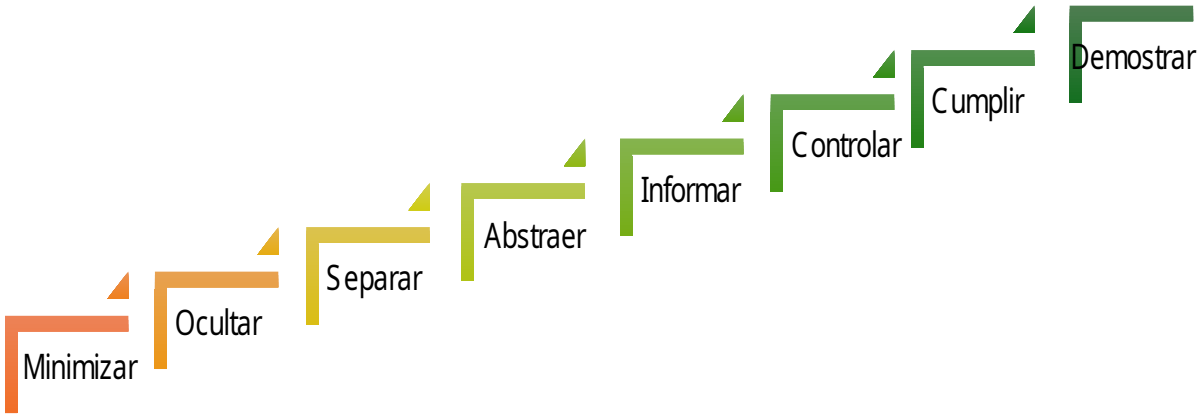
[1] LOPDP, artículo 39.

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. La arquitectura de Cero Confianza consiste en principios generales que deben ser implementados en las operaciones de desarrollo de software (DevOps) y en la configuración del software para 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 tratamiento de datos personales en tres dimensiones: privacidad (DevPrivOps), seguridad de la información (DevSecOps) y 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 los que consideren necesarios de acuerdo a las condiciones particulares del tratamiento de datos personales que realicen.

2.1. DevPrivOps

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



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

2.1.1. Minimizar. Consiste en utilizar la menor cantidad posible de datos personales, para cumplir con los fines necesarios del tratamiento. La estrategias y operaciones de minimización de datos requieren de una gestión de riesgos que aclare el panorama de los datos necesarios para cumplir con una finalidad, considerando que todo tratamiento de datos incluye riesgos, y consecuentemente, un valor al riesgo.
Tácticas. Es recomendable implementar las siguientes tácticas:

Seleccionar. Solicitar sólo datos y atributos relevantes de personas naturales. No recolectar datos personales irrelevantes,

Excluir. Excluir datos y atributos irrelevantes de personas naturales. Exluir todo lo que no ayude a cumplir con los fines lícitos del tratamiento.

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

Destruir. Eliminar datos utilizando estándares de borrado seguro, incluyendo su eliminación de las copias de respaldo (backups).

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

Tácticas. A nivel táctico, pueden utilizarse mecanismos para restringir, obfuscar, disociar, y evitar correlaciones entre los potenciales datos personales que lleguen a identificar a una persona natural. Se recomienda utilizar medidas de seguridad como el cifrado.

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

Obfuscar. Prevenir la legibilidad de los datos personales con técnicas de mejorarmiento de la privacidad, tales como esteganografía, el cifrado, y otras de la privacidad diferencial.

Disociar. Romper los vínculo entre personas naturales, eventos, y datos.

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

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

Isolar. Registrar y procesar datos personales en diferentes bases de datos, separadas de manera lógica, y/o en diferente hardware.

Distribución. Distribuir 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 posible los detalles de los datos personales que son tratados. Se diferencia de la estrategia de minimizar, en cuanto que esta estrategia se centra en los detalles con que los datos personales son tratados. A nivel táctico, abstraer datos personales requiere de evaluar el grado de detalles necesarios 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 minimizen los detalles de los datos personales tratados. Por ejemplo, agregar ruido en los datos para alterar el dato personal original.

Sumarización. Resumir los atributos particulares en atributos mas generales.

Agrupación. Procesar información acerca de un grupo de personas en lugar de información de cada persona natural en particular.

Perturbación. No exponer el valor real de los datos, sino más bien, 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. A nivel táctico, consiste en implementar las medidas organizacionales necesarias para facilitar la información a los titulares de datos sobre todo aspecto relacionado con el tratamiento de sus datos, explicar las razones por las cuales es necesario el tratamiento de datos, y notificar en tiempo real a los titulares de datos cuando los datos fuesen transferidos a terceros, o cuando haya la presunción de una vulneración de seguridad de los datos.

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

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

Notificar. Avisar a los titulares de datos cuando sus datos personales fuesen compartidos en terceros.

2.1.6. Controlar. Consiste en dar a los titulares de datos, mecanismos para controlar el tratamiento de sus datos personales. A nivel táctico, es necesario implementar mecanismos para que los titulares de datos puedan otorgar y revocar su consentimiento, escoger medidas alternativas para su consentimiento (como servicios pagados), ejercer sus derechos establecidos en la LOPDP como el derecho de rectificación, actualización,

portabilidad, eliminación, oposición, suspensión. Por ejemplo, implementar mecanismos para ejercer estos derechos que estén a disposición del titular de datos en su espacio Web, o al menos un medio de contacto como email o chat, que los ejecute con celeridad.

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

Escoger. Otorgar a los titulares de datos un consentimiento real, que no esté absolutamente condicionado por una relación de poder, o por ofrecer una recompensa económica.

Actualizar. Proveer a los titulares de datos, mecanismos para actualizar sus datos, o para solicitar la recitificación de ellos.

Retraer. Proveer a los titulares de datos, mecanismos para oponerse al tratamiento de sus datos, incluyendo la suspensión y eliminación de ellos.

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. Es necesario tener una política de protección de datos que cumpla con el deber ser, pero más importante aún, llevarlo a la práctica e implementar una gestión de riesgos para la protección de derechos y libertades con controles de riesgos implementados, eficaces y eficientes. Para ello, establecer los responsables internos que deben cumplir con cada procedimiento de seguridad organizacional y técnica. A nivel táctico, es fundamental crear una política de protección de datos personales, implementarla con los controles jurídicos, organizacionales y técnicos necesarios, y monitorear los cambios de circunstancias que pueden ocurrir, para actualizar tanto la política de protección de datos personales, como su implementación.

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

Mantener. Mantener una declaración de aplicabilidad con la justificación y descripción de medidas de seguridad organizacionales y técnicas. Implementarlos 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 que se está cumpliendo con las obligaciones establecidas en la LOPDP en la práctica. A nivel táctico, este principio requiere de registrar todos los procesos que involucren el tratamiento de datos personales, auditar todos los procesos en el ámbito jurídico, organizacional y técnico, y elaborar reportes para cumplir con los potenciales controles de la SPDP.

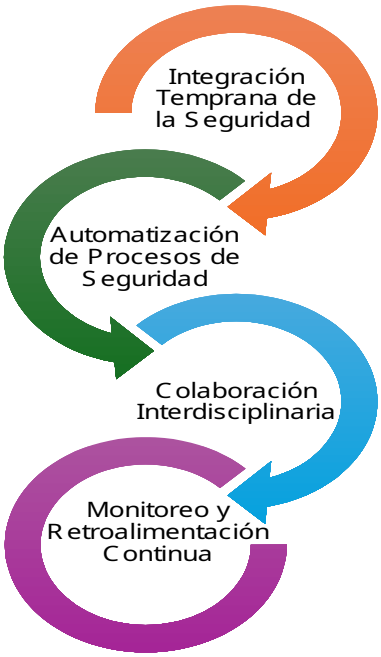
Registrar. Documentar los procesos decisionales de la institución, y guardar los registros de los tratamientos de datos personales.

Auditar. Auditar los registros de actividades del tratamiento de datos personales de manera regular y periódica, tales como registros de sgeuridad, de eventos, de errores.

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

2.2. DevSecOps

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.[5] A continuación se establecen 4 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

[5] 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.

eficiente y económica. En el contexto de la protección de datos, esto se traduce en la implementación temprana de controles como el cifrado, la autenticación robusta y la minimización de datos, asegurando que la privacidad esté integrada desde el inicio del desarrollo.

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. La automatización garantiza 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) SAST (Static Application Security Testing). 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) DAST (Dynamic Application Security Testing). 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) Software Composition Analysis (SCA). 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) Infraestructura como código (IaC) scanning. Automatiza la revisión de archivos de infraestructura como: Terraform, CloudFormation o Kubernetes para garantizar que los recursos como bases de datos, buckets de almacenamiento o redes virtuales estén configurados con políticas seguras sin exposición pública o con cifrado activado.

e) Data leakage detection. 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) Pipelines CI/CD con validaciones. Cada vez que se realice un cambio, el sistema automáticamente ejecuta todas las pruebas de seguridad anteriores antes de permitir el despliegue. Evitando que los mismos sean descubiertos en el ambiente de producción.[6]

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 y seguridad 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

[6] Ver Feio C., *et al.*, *An Empirical Study of DevSecOps Focused on Continuous Security Testing*, EuroS&PW 2024.

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 preventivas o correctivas[7]. 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 anonimización.

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

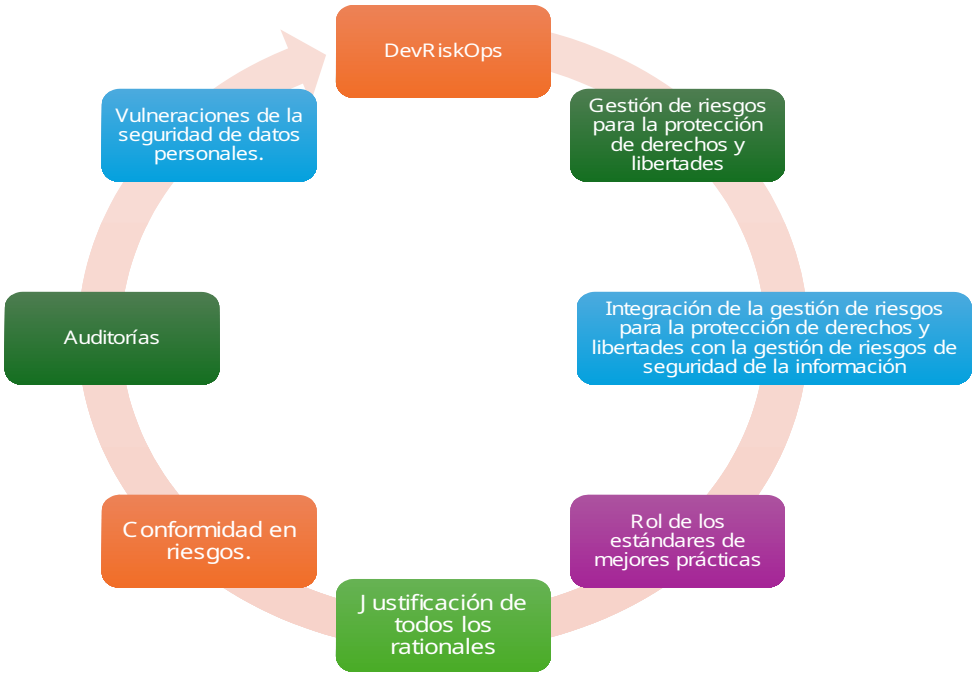
2.2.4. Monitoreo y Retroalimentación Continua. El monitoreo continuo en entornos DevSecOps constituye un elemento fundamental para la detección oportuna de vulnerabilidades, comportamientos anómalos y accesos no autorizados que puedan comprometer la seguridad de los datos personales. A través de herramientas 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 sensibles. En particular, la instrumentación de entornos con sistemas de detección de intrusos, monitoreo de logs en tiempo real y alertas automatizadas constituye una práctica esencial para garantizar la trazabilidad, la rendición de cuentas y la protección efectiva de la información.[8]

2.3. DevRiskOps

Dado que la LOPDP se fundamenta en la gestión de riesgos, es importante considerar los principios de la gestión de riesgos 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 ya definidos en la *Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales*, pero a nivel macro-estratégico, en el contexto de la protección de datos desde el diseño y por defecto.

[7] 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.
[8] Prates L. y Pereira R., *DevSecOps practices and tools*. *International Journal of Information Security*, 2024.



2.3.1. Gestión de riesgos para la protección de derechos y libertades. Este principio consiste en enfocarse en 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 determinar si es necesario realizar una evaluación de impacto del tratamiento de datos personales, en función de haber elaborado y comparado escenarios de riesgos probables contra los derechos y libertades de los titulares de datos. Se recomienda realizar por defecto una gestión de riesgos para la protección de derechos y libertades futuros, e implementar el principio de protección de daños desde el diseño y por defecto en función de las operaciones DevPrivOps y DevSecOps.

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 derechos y libertades de los titulares de 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 determinar las mejores guías y estándares para las operaciones DevPrivOps y DevSecOps, que pueden guiar 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 implementación del principio de protección de datos desde el diseno y por defecto. En este contexto, y en lugar de analizar el riesgo inherente de un sistema que involucre de tratamiento de datos personales, se trata de justificar los valores de entrada y criterios utilizados en la implementación de las operaciones DevPrivOps y DevSecOps. Es fundamental implementar 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 la conformidad en papel, sino más bien tener una lógica de identificación, análisis y evaluación de riesgos desde la concepción 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 riesgos, lo cual ayude al responsable del tratamiento a seleccionar e implementar las operaciones mas 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 impacto 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. Se recomienda evaluar los futuros riesgos considerando por separado las tres dimensiones de la seguridad de datos personales: confidencialidad, integridad y disponibilidad.

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 tener un modelo que permita calificar el grado de madurez que tenga un responsable del tratamiento de datos en la implementación de estos principios. La permeabilidad de los principios es una misión continua y de tracto sucesivo, por la cual los responsables del tratamiento ganarán la experiencia para futuros proyectos que involucren el tratamiento 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. Este mismo 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.
Nivel 1 – Implícito. El principio es conocido y asumido como necesario, pero ha sido implementado en menos del 25% del proceso.
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.
Nivel 3 – Maduro explícito. El principio es conocido, asumido como necesario y ha sido implementado en más del 75 % del proceso.

La estimación de cada principio para una actividad de tratamiento de datos personales debe tener un rationale cuantitativo o cualititativo, 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 derechos y libertades servirán para calibrar de manera adecuada todos lo 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 que permita poder identificar y clasificar todos los procesos que involucran el tratamiento de datos personales. Este registro deberá contener de manera granular cada tratamiento de datos personales que se realiza. El total de procesos de tratamiento de datos personales constituye el espacio de sampleo. Ejemplo:

REGISTRO DE ACTIVIDADES DEL TRATAMIENTO EN UN COLEGIO

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

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 (cuando no haya datos o métricas significativas). El principio debe estar respaldado por los correspondientes controles de riesgos que sean eficaces y eficientes. No obstante, se puede que un principio se haya implementado parcialmente, para lo cual se puede utilizar el nivel de madurez correspondiente. Se pueden utilizar tablas para el registro de evaluación:

ACTIVIDAD DEL TRATAMIENTO : Registro de matrículas de estudiantes

DevPrivOps

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

DevSecOps

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

DevRiskOps

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

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 todos en conjunto. No obstante, esta evaluación de nivel de madurez es a nivel estratégico en cuanto a permeabilidad de los principios correspondientes a los ejes de DevPrivOps, DevSecOps, y DevRiskOps. Una vez que ya haya implementación, 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 en función de los resultados obtenidos.

3.3.1. Nivel de madurez de todos los principios juntos. Es un sistema cualitativo similar al ya presentado para evaluar la implementación de cada principio en una actividad de tratamiento de datos en particular, pero con el objetivo de analizar a todos los procesos juntos, que involucren el tratamiento de datos personales. Se recomienda el 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.

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, en que un Colegio es el responsable del tratamiento de datos, y tiene 10 Actividades de Tratamiento de Datos Personales. EDS = 10.

b) Evaluación global de todos procesos (EGP). Es la calificación global asignada a los procesos que involucran el tratamiento de datos personales, en caja uno de los ejes. Del ejemplo anterior podemos representar cuantos están en nivel caótico, en nivel implícito, en nivel temprano explícito, y el nivel maduro explícito. Podemos estimar el total de los niveles de un mismo principio en las 10 actividades del tratamiento.

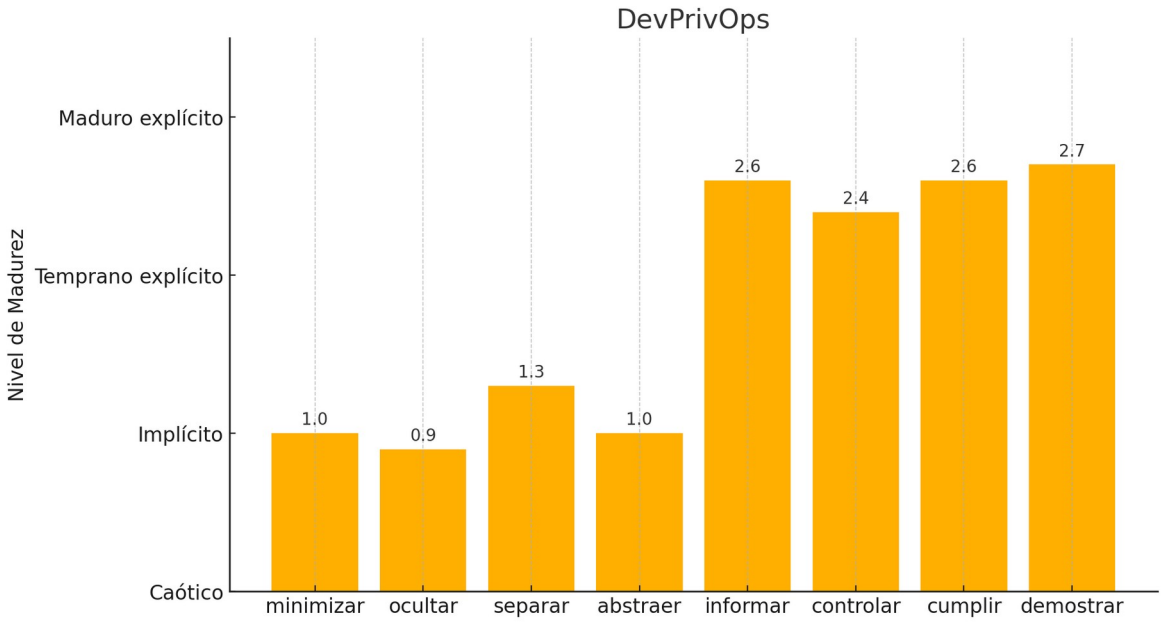
Array DevPrivOps = [minimizar, ocultar, separar, abstraer, informar, controlar, cumplir, demostrar]

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

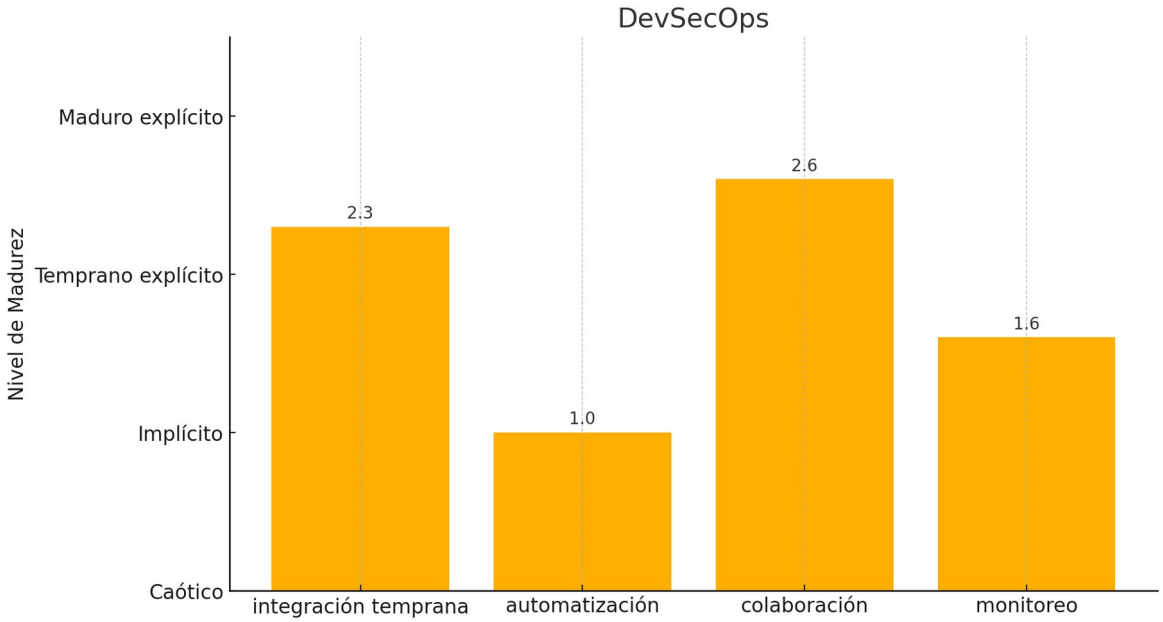
Array DevriskOps = [gestión de riesgos para protección de derechos y libertades, integración con la seguridad de la información, estándares de mejores prácticas, rationales, conformidad en riesgos, auditorías, prevención de vulneraciones de seguridad]

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, 2]	[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, 4]	[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]

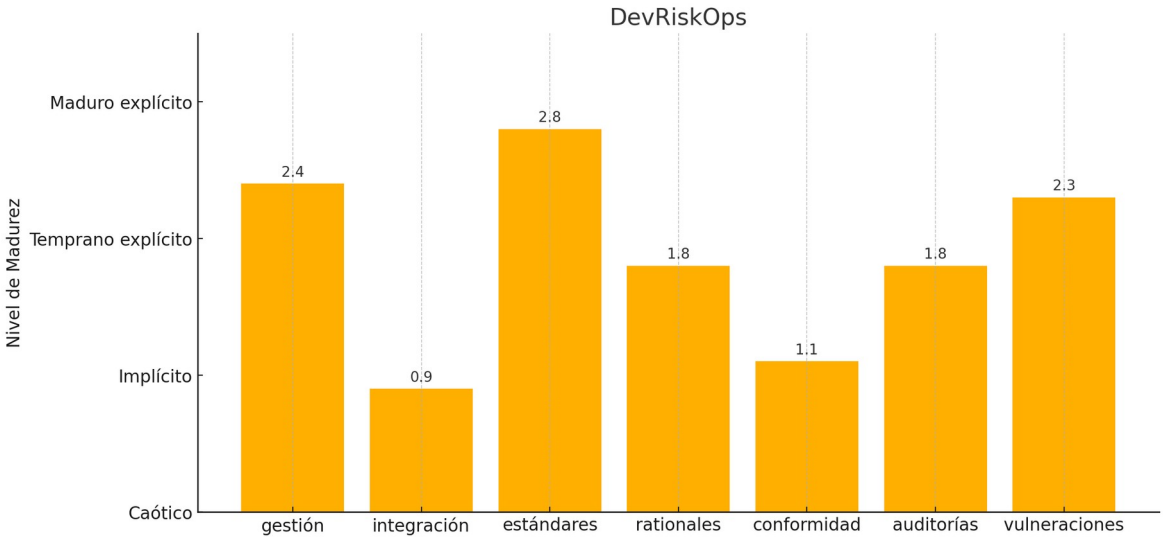
Nivel de madurez DevPrivOps = [minimizar (1.0), ocultar (0.9), separar (1.3), abstraer (1.0), informar (2.6), controlar (2.4), cumplir (2.6), demostrar (2.7)]



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



Nivel de madurez DevRiskOps = [gestión de riesgos para la protección de 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), auditorias (1.8), prevención de vulneraciones (2.3)]



SUPERINTENDENCIA DE PROTECCIÓN DE DATOS PERSONALES

Av. Amazonas y Unión Nacional de Periodistas. Plataforma Gubernamental
de Gestión Financiera. Bloque Amarillo, piso 4.
Quito – Ecuador

www.spdp.gob.ec