

PERSPECTIVAS BF

UNA MIRADA AL MUNDO LEGAL

Delegado de Protección de Datos Personales (DPO): **La Nueva Columna Vertebral del Cumplimiento Corporativo en Ecuador**



**BUSTAMANTE
FABARA**

ECUADOR | WWW.BUSTAMANTEFABARA.COM



Delegado de Protección de Datos Personales (DPO): La Nueva Columna Vertebral del Cumplimiento Corporativo en Ecuador

El avance de la transformación digital, la consolidación de modelos de negocio basados en datos y la creciente preocupación mundial por la privacidad, han provocado que las organizaciones revisen, cuestionen y reestructuren sus prácticas internas. En Ecuador, esta evolución se materializa con la entrada en vigor del Reglamento del Delegado de Protección de Datos Personales (DPO), una figura que se convertirá en un pilar imprescindible para el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPD).

La normativa establece que, a partir del **1 de noviembre de 2025**, las entidades obligadas deberán **designar e inscribir oficialmente a su DPO** ante la Superintendencia de Protección de Datos Personales (SPDP). Ese hito, más que un trámite, inaugura una nueva etapa en la gestión empresarial: una en la que la privacidad, la transparencia y la responsabilidad adquieren un rol protagónico. El plazo final para inscribir al DPO ante la SPDP vence el 31 de diciembre de 2025.

Un Rol que Transforma la Estructura Interna

La figura del Delegado de Protección de Datos Personales no solo cumple una función técnica, sino también estratégica. Su rol es

garantizar que los datos personales dentro de una organización se manejen con criterios de legalidad, seguridad y respeto a los derechos de los titulares.

A diferencia de otras responsabilidades que pueden diluirse entre varias áreas, el DPO debe cumplir funciones claramente definidas: supervisar el cumplimiento de la organización sobre la normativa de protección de datos, asesorar en la ejecución del análisis de riesgo y las evaluaciones de impacto, garantizar la aplicación de políticas de privacidad, responder ante incidentes de seguridad y gestionar la atención del ejercicio de derechos de los titulares.

Todo ello exige una visión transversal del negocio y un entendimiento profundo de los procesos corporativos, la tecnología empleada y el marco jurídico aplicable. La designación de un DPO implica necesariamente una revisión interna. Muchas organizaciones se verán forzadas a actualizar procedimientos, reorganizar flujos y aclarar responsabilidades.

La privacidad deja de ser una tarea aislada del departamento de sistemas o legal: pasa a ser un esfuerzo conjunto que involucra a las áreas comerciales, de compliance, tecnología, talento humano y alta dirección.

"El DPO es el guardián interno de la privacidad y el enlace directo con la autoridad reguladora."

¿Quiénes deben adoptar esta figura?

El Reglamento del DPO identifica **14 sectores obligados** a contar con esta figura. Instituciones educativas, entidades financieras, aseguradoras, laboratorios farmacéuticos, hospitales y empresas del sector salud, empresas de seguridad privada, telecomunicaciones, publicidad digital y proveedores de videovigilancia masiva son solo algunos ejemplos. No es casualidad: estos sectores operan con volúmenes de datos especialmente delicados y necesitan un mayor estándar de supervisión.

Para estas organizaciones, el DPO no solo es un requisito legal, sino un componente esencial para preservar la confianza. En tiempos donde las brechas de seguridad y el uso indebido de datos se convierten en riesgos reputacionales de alto impacto, contar con un profesional especializado es un factor diferencial. El DPO se convierte así en un gestor de riesgo, un asesor estratégico y un garante de buenas prácticas.

Riesgos de incumplir: un costo mayor que una multa

La normativa es clara: no inscribir un DPO cuando corresponde constituye una **infracción grave**, sancionada con multas que pueden alcanzar hasta el **1% de los ingresos del año anterior**. Sin embargo, el verdadero costo del incumplimiento va más allá de una sanción económica.

Una brecha de datos, un incidente no reportado a tiempo o un proceso interno mal documentado puede provocar consecuencias irreversibles. Pérdida de confianza, deterioro de la reputación, afectación a relaciones comerciales y eventuales acciones legales son escenarios posibles. En el contexto actual, donde la transparencia es un activo reputacional, la ausencia de un DPO envía un mensaje de vulnerabilidad.

El Delegado de Protección de Datos es, por tanto, una pieza clave en la prevención. Su labor continua y multidisciplinaria reduce la probabilidad de incidentes, fortalece los controles internos y permite anticipar riesgos que, en otras circunstancias, pasarían desapercibidos.





Una función especializada: más allá del título profesional

El Reglamento exige que el DPO cumpla requisitos específicos que garantizan su idoneidad. Debe ser mayor de edad, estar en goce de sus derechos políticos, poseer un título de tercer nivel en Derecho, Sistemas de Información, Comunicación o Tecnologías y contar con al menos cinco años de experiencia profesional verificable. Además —y este punto es decisivo— deberá de aprobar un programa profesionalizante ofrecido por una institución de educación superior que sea acreditada por la SPDP.

La responsabilidad del DPO implica un conocimiento profundo del marco jurídico, pero también del funcionamiento tecnológico de los sistemas y de los riesgos asociados al entorno digital. La convergencia entre lo legal y lo técnico requiere un perfil

híbrido: un profesional que cuente con criterio jurídico, entendimiento técnico y habilidades de gestión.

Transformación Cultural y Actualización de Procesos

La incorporación del DPO no es un acto aislado. Requiere —como ocurrió con la transición a juntas y firmas 100% virtuales— un proceso de adaptación interna que involucra a toda la organización. Se trata de revisar protocolos, actualizar contratos con proveedores, redefinir matrices de riesgo, implementar una serie de controles técnicos y reorganizar la documentación interna.

Pero, quizá lo más importante, implica **crear una cultura de privacidad**. Esta cultura debe permear todos los niveles: desde los colaboradores que manejan información sensible a diario hasta los ejecutivos que toman decisiones estratégicas. La privacidad no puede ser vista como una carga; debe

interpretarse como una capa de valor, una ventaja competitiva y un compromiso ético.

Conclusión: Anticiparse es Liderar

El marco normativo ecuatoriano finalmente se alinea con los estándares globales de protección de datos. Las organizaciones que adopten —de manera temprana— buenas prácticas y diseñen un DPO competente estarán mejor posicionadas para enfrentar los desafíos del entorno digital.

El designar e inscribir al Delegado de Protección de Datos Personales no solo es cumplir una obligación legal: es asumir un compromiso con la transparencia, la confianza y la responsabilidad corporativa. Las compañías que se anticipen no solo evitarán sanciones, sino que fortalecerán su reputación y consolidarán una ventaja competitiva en un mercado cada vez más orientado a la ética empresarial.

Nuestro equipo

En **BUSTAMANTE FABARA**, nuestro equipo especializado en Protección de Datos Personales brinda asesoría integral para la **designación, registro y cumplimiento** del DPO, acompañando a las organizaciones en cada etapa del proceso.



María Rosa Fabara Vera
MANAGING PARTNER

Con más de 25 años de experiencia, presta asesoría jurídica permanente a clientes nacionales y extranjeros, principalmente en temas relacionados con fusiones y adquisiciones, asuntos regulatorios, corporativos, contratación pública, alianzas público-privadas, y en las áreas de competencia económica y propiedad intelectual.

Amplia experiencia en la asesoría jurídica a los sectores farmacéutico, seguros y de medicina prepagada, construcción, infraestructura, financiación de proyectos, entre otros. Cuenta con una destacada y reconocida experiencia en el área de Propiedad Intelectual, especialmente en marcas, patentes, derechos de autor, nuevas tecnologías, y competencia desleal.



Esteban Dávila Caicedo
ASOCIADO SÉNIOR

Esteban concentra su práctica en asuntos relativos al derecho de competencia o antitrust, protección de datos personales y compliance.

Entre sus actividades, están las de defensa de clientes en complejos procedimientos administrativos ante la autoridad de competencia local, por: prácticas desleales, prácticas de abuso de poder de mercado, acuerdos restrictivos y asesoría en importantes concentraciones económicas de compañías nacionales e internacionales. También, asesora a clientes en procesos de implementación de la normativa de protección de datos personales; y, en general, de programas de compliance.



Rafael Gabela Salvador
ASOCIADO

Como parte del equipo de BUSTAMANTE FABARA, ha participado en la implementación de programas de protección de datos personales en empresas del sector asegurador, medicina prepagada, retail, financiero, bancario y automotriz.

Además de participar en la implementación de estos programas, Rafael ha desarrollado políticas específicas de protección de datos personales. Su experiencia incluye asesoramiento en gestión de riesgos y prevención de brechas de seguridad de la información, así como el diseño e implementación de procedimientos para garantizar el ejercicio efectivo de los derechos de los titulares de datos personales.

Quito - Ecuador
Av. Patria E4-69 y
Amazonas
Edificio COFIEC
T. +593 2 256 2680

Guayaquil - Ecuador
Av. de Alarcón y Av. de las
Américas
Edif. Sky Building
Piso 4, Of. 423
T. +593 2 256 2680 ext 1901

ECUADOR
www.bustamantefabara.com

