

CONSULTORÍA

Esquema Metodológico para Evaluación de Confidencialidad y Protección de Datos



www.desoal.org

Impacto metodológico institucional

Copyright © DESOAL-ORG 2026

En el marco legal ecuatoriano, la potestad de "Auditoría" es una facultad administrativa de control exclusiva de la Superintendencia de Protección de Datos Personales (SPDP); sin embargo, la norma autoriza que empresas consultoras pertinentes realicen procesos de validación integral adecuados para dicho ámbito de evaluación certificada de cumplimiento normativo.

El esquema metodológico de DESOALORG permite evaluar la madurez de la empresa desde su alta gerencia hasta sus activos críticos, emitiendo los documentos de respaldo necesarios para su cliente requirente y/o entidad rectora que realicen control de seguimiento normativo.

Fase I: Evaluación de Gobernanza Institucional

(Nivel Orgánico y Normativo)

Objetivo: Determinar si la estructura superior y las normas internas de la empresa están diseñadas para garantizar la seguridad y privacidad desde la raíz.

1.1. Evaluación del Compromiso de la Alta Dirección: Revisión de planes estratégicos donde se incluya la seguridad de la información como prioridad institucional.

1.2. Validación de la Estructura Orgánica: Verificación de la creación de roles específicos: Responsable de Seguridad, Comité de Privacidad o designación del Delegado de Protección de Datos (DPD).

- Evaluación de la segregación de funciones para evitar conflictos de interés en el manejo de datos.

1.3. Evaluación del Marco Normativo Interno: Análisis de Reglamentos Internos de Trabajo, Códigos de Ética y Manuales de Procedimientos.

- Validación de la Política Marco de Seguridad de la Información, Protección de Datos y su socialización oficial en la empresa.
- Revisión de políticas que consideren manejo de documentos impresos, registros digitales, políticas de "Escritorio Limpio" y "Pantalla Bloqueada".
- Verificación de roles de custodia, responsabilidades asignadas para la administración de llaves, archivos centrales y bodegas de documentos.
- Revisión de cláusulas con proveedores y clientes, respecto a Contratos y Confidencialidad.

1.4. Insumos Requeridos: Al menos, Escrituras de constitución, Organigrama, Reglamento Interno de Trabajo, Políticas Institucionales de Confidencialidad y Tratamiento de Datos (en físico, digital y sistemas), Manuales de Funciones, Manuales de Operaciones en gestión con Clientes y Proveedores.

“Hoja de Ruta en 4 fases para Evaluación y Validación Integral orientado al Fortalecimiento de Confidencialidad y Protección de Datos”

DESOAL-ORG

Fase II: Evaluación Técnica y Operativa

(Activos e Información)

Objetivo: Validar la aplicación práctica de los lineamientos institucionales en los flujos de datos (impresos, manuscritos, digitales), archivos físicos y sistemas tecnológicos.

2.1. Inventario y Ciclo de Vida del Dato: Identificación de activos (archivos físicos, software, hardware, nubes), mapeo del flujo de datos personales en el marco de los procesos de gestión institucional, y procedimientos para cumplir con su retención, integridad, integralidad, manejo de uso y archivístico (físico, digital, informático).

2.2. Validación de Medidas Técnicas: Evaluación de los controles de seguridad implementados (clasificación de confidencialidad, control archivístico de documentos físicos, gestión digital, controles de acceso, cifrado, autenticación multifactor, copias de seguridad, protecciones físicas y tecnológicas, etc.).

2.3. Evaluación de Riesgos Operativos: Identificación de amenazas que puedan comprometer la confidencialidad de la información gestionada para terceros.

Fase III: Validación de Resultados y Emisión de Documentación de Respaldo

Objetivo: Generar los documentos que avalen ante la empresa requirente (cliente) que la empresa en calidad de proveedor ha pasado por un proceso riguroso de validación externa.

Entregables de Aval (a ser emitidos por DESOALORG S.A.S.):

1. Informe de Gap Analysis Integral: Detalle de brechas digitales, tecnológicas y vulnerabilidades detectadas en la gestión documental física.
2. Informe de Evaluación de Cumplimiento Integral: Detalla el estado de la empresa en los niveles Orgánico, Normativo y Técnico (en complemento al Gap Analysis Integral).
3. Certificado de Validación de Proceso: Documento firmado por la consultora que avala que la empresa proveedora ha sido evaluada y cuenta con un sistema de gestión en marcha y un Plan de fortalecimiento institucional.

4. Dossier de Responsabilidad Proactiva: Compendio de evidencias (políticas, RAT [Registro de Actividades de Tratamiento], planes de seguridad, etc.) para entrega inmediata al cliente requirente.

Fase IV: Hoja de Ruta de Aplicación de Acciones

(Remediación)

Objetivo: Establecer el plan de trabajo para cubrir los gaps identificados en la evaluación inicial y alcanzar el cumplimiento pleno; tales como pueden ser:

Nivel de Acción	Descripción de la Acción de Remediación	Prioridad
Orgánico	Formalización del Comité de Seguridad de la Información y Protección de Datos.	Muy Alta
Normativo	Actualización de contratos con terceros, cláusulas de confidencialidad laboral, actualización del Manual de Gestión Documental Física y Digital y del Manual de Gestión de Datos Sistematizada con criterios de Protección de Datos.	Alta
Político	Creación y aprobación de la Política de Retención y Destrucción Segura de Datos.	Alta
Archivístico	Implementación de instalaciones, mobiliario y protocolos para gestión documental física, que incluya la Destrucción Segura (Art. 15 LOPDP).	Crítica
Tecnológico	Implementación de protocolos de cifrado y endurecimiento de arquitecturas o servidores TI (Hardening – reducción de vulnerabilidades).	Crítica
Operativo	Programa de capacitación continua y simulacros de incidentes de seguridad con información física, digital o sistematizada.	Media

Sustento Normativo de la Evaluación y Validación por DESOALORG S.A.S.

La metodología de **Evaluación de Cumplimiento y Validación Técnica** encuentra su fundamento legal en el **Principio de Responsabilidad Proactiva (Accountability)**, consagrado en el **Art. 33 de la Ley Orgánica de Protección de Datos Personales (LOPDP)** de Ecuador, el cual obliga a los responsables y encargados a implementar mecanismos que demuestren fehacientemente la adopción de medidas técnicas, organizativas y jurídicas para garantizar la protección de datos.

Dado que la LOPDP exige en su **Art. 53** la implementación de medidas de seguridad proporcionales al riesgo, cuya efectividad debe ser **verificada, evaluada y valorada periódicamente**, el diagnóstico de brechas y los

informes de validación emitidos por consultoras especializadas se constituyen como instrumentos de gestión válidos y legalmente reconocidos. Estos documentos certifican la **debida diligencia** de la organización, sirviendo como evidencia objetiva de cumplimiento ante terceros y la Autoridad de Protección de Datos, conforme lo previsto en el **Art. 47, numeral 10**, que permite la contratación de servicios de apoyo externo para la gestión de la seguridad, y en concordancia con el deber de confidencialidad y sigilo exigido en el **Art. 3, literal h** de la citada norma.

Debido a la naturaleza específica de los activos críticos y el flujo de datos de cada organización o empresa, el alcance final, el cronograma de trabajo y la valoración económica del servicio serán definidos tras una sesión técnica de diagnóstico preliminar.

DESOAL-ORG

La ejecución de esta consultoría bajo la metodología de **DESOAL-ORG** representa para su organización o empresa una inversión estratégica en **seguridad jurídica y reputacional**, garantizando que el cumplimiento normativo se transforme en una ventaja competitiva. Al implementar este esquema de cuatro fases, su organización no solo mitiga riesgos operativos y vulnerabilidades técnicas, sino que adquiere la capacidad de demostrar **Responsabilidad Proactiva (Accountability)** mediante entregables de alto valor, como el **Dossier de Evidencias** y el **Certificado de Validación**. Estos instrumentos constituyen la prueba objetiva de debida diligencia requerida por el Art. 33 de la LOPDP ante clientes, proveedores y la Autoridad de Protección de Datos.

Más allá del cumplimiento legal, este proceso fortalece la confianza de los grupos de interés de las empresas, y asegura la continuidad del negocio mediante una gestión documental y digital blindada, eficiente y alineada con los más altos estándares de confidencialidad y sigilo alineada con la normativa vigente.



Mgtr. Marcelo Carrera Riquetti

Gerente General / CEO

DESOALORG S.A.S.

ceo@desoal.org

Móvil / WhatsApp: +593 996158303

www.desoal.org

Quito – Ecuador