50 AÑOS CORRAL ROSALES

DGRV
Confederación Alemana de Cooperativas

Capacitación en Protección de Datos Personales

Sesión 2

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

Medidas de seguridad

Seguridad de datos personales: dependerá de la categoría y volumen de los datos, estado de la técnica y costos de aplicación.

¿Qué se debe implementar?

Procesos de verificación, evaluación y valoración continua – evidenciar las medidas adoptadas e implementadas.

Ejemplo de medidas:

i. Anonimización, cifrado de datos
ii. Confidencialidad, integridad y disponibilidad permanente.
iii. Medidas técnicas, físicas, jurídicas, organizativas.

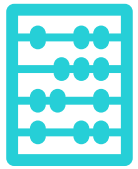
Análisis de Riesgos - Determina las medidas de seguridad:

i. Particularidades del tratamiento
ii. Partes involucradas.
iii. Categorías y volúmenes de datos.

Medidas de seguridad

Seguridad de datos personales: Para determinar las medidas de seguridad, se deberán tomar en consideración, como mínimo, las siguientes:

- **Los resultados del análisis de riesgos, amenazas y vulnerabilidades.**



- **Naturaleza de los datos personales.**

- **Características de las partes involucradas.**

- **Antecedentes de destrucción de los datos personales.**

Análisis de riesgo

Riesgo: Posibilidad de que se materialice una amenaza y sus consecuencias negativas.

Análisis de Riesgo

Metodología que permite **identificar el nivel de riesgo** de los tratamientos de datos personales para determinar las medidas de seguridad y garantizar los derechos y libertades de los titulares.

¿Qué se necesita para realizar un Análisis de Riesgo?

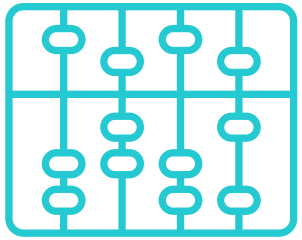
1. Registro de Actividades de Tratamiento (RAT).
2. Contar con una metodología que permita mitigar el riesgo.

¿Qué se debe hacer si el análisis de riesgo tiene como resultado un riesgo alto?

Realizar una Evaluación de Impacto.

Evaluación de Impacto

Análisis preventivo que para valorar los impactos reales del tratamiento con el fin de determinar y mitigar posibles vulneraciones de derechos y libertades antes de que se materialicen.



¿Cuándo se debe realizar una Evaluación de Impacto?

1. Previo al inicio del tratamiento.
2. Cuando el tratamiento sea de alto riesgo para los derechos y libertades del titular.
3. Cuando la Autoridad lo requiera.

Requisitos para las Evaluaciones de Impacto

i. Descripción del tratamiento.
ii. Evaluación de su necesidad y proporcionalidad respecto de la finalidad.
iii. Evaluación de los riesgos y libertades de los titulares.
iv. Medidas para reducir o mitigar el riesgo.

DGRV
Confederación Alemana de Cooperativas

Pasos a seguir para una correcta aplicación de medidas de seguridad

CORRAL ROSALES 50 AÑOS

1. Verificar que se tenga un **Registro de Actividades de Tratamiento** actualizado.

2. Realizar un **Análisis de Riesgo** a todas las actividades de tratamiento de datos personales.

3. Realizar la **Evaluación de Impacto** a los tratamientos aplicables.

Establecer un **plan** para implementar controles con el fin de reducir el nivel riesgo.

Aplicar medidas de seguridad para disminuir la probabilidad o el impacto de los riesgos.

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

Medidas de seguridad a implementar

Administrativas

Procedimientos de gestión de incidentes de seguridad, protocolos de acceso y eliminación de datos personales

Técnicas

Cifrado de datos, firewalls y antivirus, autenticación de múltiples factores, copias de seguridad y almacenamiento seguro.

Físicas

Controles de acceso, resguardo de la información física y digital, protección y mantenimiento de equipos.

Jurídicas

Políticas de privacidad y avisos de confidencialidad; contratos y acuerdos de confidencialidad (NDA), etc.

Organizativas

Designación de un Delegado de Protección de Datos, Programas de concienciación y formación en protección de datos para empleados

Vulneraciones de seguridad

¿Cuándo nos encontramos frente a una vulneración de seguridad?

- Datos personales fueron destruidos, no existen o dejan de estar disponibles para el Responsable.
- Tratamiento no ha sido autorizado o es ilícito, incluyendo la divulgación o acceso no autorizados por parte de destinatarios.
- Datos personales fueron alterados, corrompidos o no son íntegros.
- Responsable ha perdido el control o acceso, o los datos personales ya no están en su poder.

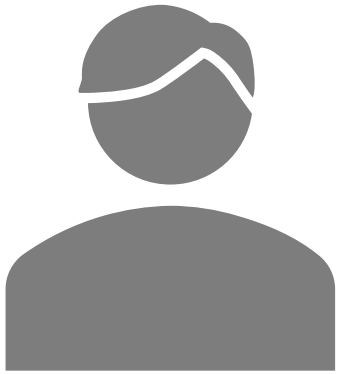
Notificaciones de vulneraciones de seguridad

A la Autoridad

Superintendencia de Protección de Datos Personales y ARCOTEL

- En un término de **5 días** desde que se tenga constancia de la vulneración. – Explicar motivos si no se hace en ese plazo.
- Excepto si es improbable que dicha violación constituya un riesgo para los derechos y libertades.

Encargado debe notificar al Responsable en un plazo de 2 días



Al Titular (socio)

Se debe notificar al socio en el término de **3 días** cuando exista un riesgo a derechos y libertades fundamentales.

No se debe notificar cuando:

- Se hayan adoptado las medidas de protección (calificada por la autoridad).
- Se hayan adoptado medidas que garanticen que el riesgo a los derechos no ocurrirá. (Calificada por la Autoridad).
- Implica un esfuerzo desproporcionado hacerlo – comunicación pública.

Régimen sancionador

Superintendencia de Protección de Datos Personales (“SPDP”)

Órgano de control y vigilancia encargado de garantizar a todos los ciudadanos la protección de sus datos personales.

Atribuciones:

i. Ejercer potestad sancionadora.
ii. Ejercer supervisión, control y evaluación.
iii. Realizar auditorías técnicas al tratamiento de datos
iv. Crear y dirigir el Registro Nacional de Protección de Datos.
v. Dictar cláusulas estándar de protección de datos .
vi. Establecer directrices para el análisis y evaluación de medidas de seguridad.

Régimen sancionador

Infracciones más comunes que los responsables pueden recaer:

Infracciones leves (multa de 0.1% a 0.7%)

- Elegir un encargado que no ofrezca garantías suficientes.
- Incumplir las medidas correctivas dispuestas por la SPDP.

Infracciones graves (multa de 0.7% a 1%)

- No implementar medidas de seguridad adecuadas.
- Comunicar datos sin cumplir los requisitos y procedimientos establecidos por la SPDP.
- No realizar análisis de riesgos ni evaluaciones de impacto.
- No notificar a la SPDP y al titular de vulneraciones de seguridad de los datos personales.
- No suscribir contratos que incluyan cláusulas de confidencialidad y tratamiento de datos personales.
- No designar un Delegado cuando corresponda.

Nota: la multa se calculará sobre el volumen de negocio de la COAC.

Régimen sancionador

Infracciones comunes

Infracciones leves (multa de 0.1% a 0.7%)

- Elegir un encargado que no ofrezca garantías suficientes.
- Incumplir las medidas correctivas dispuestas por la SPDP.

Infracciones graves (multa de 0.7% a 1%)

- No implementar medidas de seguridad adecuadas.
- Comunicar datos sin cumplir los requisitos y procedimientos establecidos por la SPDP.
- No realizar análisis de riesgos ni evaluaciones de impacto.
- No notificar a la SPDP y al titular de vulneraciones de seguridad de los datos personales.
- No suscribir contratos que incluyan cláusulas de confidencialidad y tratamiento de datos personales.
- No designar un Delegado de Protección de Datos Personales.

¿Sobre qué se calcula la multa?

La multa se calculará sobre el volumen de negocio del responsable.

Ahora bien, el volumen de negocio se entiendo a la cuantía resultante de la prestación de servicios realizado por el responsable durante el último ejercicio fiscal previa deducción de IVA y otros impuestos relacionados con la operación económica.

Régimen sancionador

La SPDP podrá imponer medidas correctivas y multas en virtud de incumplimientos a la LOPDP.

Medidas correctivas

Medidas correctivas podrán incluir:

i. Cese de tratamiento (condiciones y plazos).
ii. La eliminación de los datos.
iii. Imposición de medidas técnicas, jurídicas, organizativas o administrativas.

Multas

Las multas oscilan entre el **0,1%** y el **1%** del total de volumen de negocio del infractor por cada infracción cometida.

Las sanciones se producen por el cometimiento de infracciones leves o graves.

Importancia del cumplimiento de la normativa de protección de datos personales

Evaluación

Los datos personales son considerados activos intangibles. Por ello es necesario protegerlos de la mejor manera posible.

Evitar Sanciones

Los incumplimientos a la LOPDP son sancionados con medidas correctivas y multas de entre el 0.1% y el 1% del volumen del negocio de la COAC.

Reputación

El tratamiento inadecuado de datos personales puede resultar en daños reputacionales para la COAC.

Evitar perjuicios

Un tratamiento sin las medidas de protección necesarias podría conllevar perjuicios para los socios (ej: filtración de sus finanzas)

Importancia del cumplimiento de la normativa de protección de datos personales

Riesgos legales

Reduce la probabilidad de sanciones, multas y daños a la imagen institucional por incumplimientos normativos.

Diferenciador

Destaca nuestro compromiso y marca un diferenciador en la calidad de los servicios.

Confianza

Demuestra compromiso con la privacidad y seguridad de los datos, generando confianza entre socios y empleados.

Responsabilidad Proactiva

Fomenta una actitud preventiva frente a incidentes de seguridad y tratamiento indebido de datos.

DGRV
Confederación Alemana de Cooperativas

Pasos para el cumplimiento de la normativa en protección de datos personales

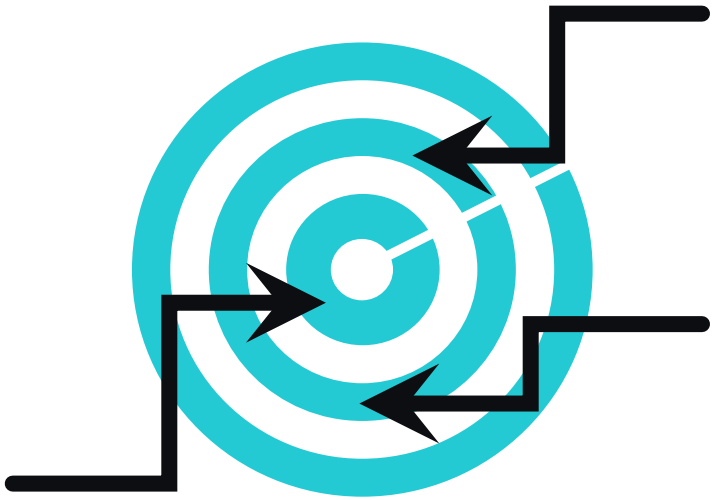
50 AÑOS CORRAL ROSALES

¿Qué es lo mínimo que se debe implementar?

Documentos / Procedimientos	
Contar con Políticas de Protección de Datos Personales.	Procedimiento de conservación y eliminación de datos personales.
Avisos de privacidad en canales digitales.	Política y proceso para integrar la privacidad por diseño y por defecto.
Avisos de videovigilancia de conformidad con la LOPDP.	Acuerdos de confidencialidad.
Mecanismo para la gestión de derechos.	Plan de capacitación para el personal en protección de datos personales.
Proceso para la atención de solicitudes de ejercicio de derechos.	Registro de Actividades de Tratamiento.
Proceso para la gestión de incidentes de seguridad.	Cláusulas de protección de datos personales.
Política de Seguridad de la Información.	Autorizaciones y declaraciones de conformidad con la LOPDP.

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

Pasos para el cumplimiento de la normativa en protección de datos personales



Identificar

Aprender a identificar las actividades de tratamiento y sus elementos relacionados.

Registro de Actividades de Tratamiento

Aprender a documentar un Registro de Actividades de Tratamiento.

Medidas Adicionales

Identificar otras medidas de cumplimiento aplicables en virtud de las actividades que ejecutamos.

Registro de Actividades de Tratamiento (“RAT”)

01	02	03	04
¿En qué operaciones o actividades usamos datos personales?	¿Para qué estamos usando esos datos personales?	¿Qué categorías de datos estamos usando en esa actividad?	¿Por qué tratamos esos datos personales?

Para identificar y documentar el tratamiento de datos personales debemos hacernos las siguientes preguntas:

05	06	07	08
¿Creamos un perfil con esos datos personales?	¿Enviamos esos datos a un tercero?	¿Requerimos de servicios de terceros para esta actividad?	¿Qué medidas de seguridad se han implementado?

Actores en el Sistema de Protección de Datos Personales

¿En qué operaciones o actividades usamos datos personales?

¿Qué se debe identificar?

Las tareas o procesos específicos donde se recolectan, almacenan, usan, consultan, modifican o eliminan datos personales.

Ejemplos comunes:

Registro de clientes, activación de servicios, envío de promociones, gestión de reclamos.

¿Cómo se registra en el RAT?

"Registro de socios."

¿Requerimos de servicios de terceros para esta actividad?

¿Qué se debe definir?

La finalidad del tratamiento: el propósito específico y legítimo por el cual se usan los datos.

Ejemplos comunes:

Cumplir con un contrato, Atender solicitudes de servicio, etc.

¿Cómo se registra en el RAT?

"Contacto y envío de información comercial."

Actores en el Sistema de Protección de Datos Personales

¿Qué categorías de datos estamos usando en esa actividad?

¿Qué se debe identificar?

Las categorías y tipos de datos personales tratados, incluyendo si se tratan de datos sensible.

¿Cómo se registra en el RAT?

"Datos de identificación: Nombre, cédula.
Datos de contacto: correo electrónico, número de teléfono."

¿Por qué tratamos esos datos personales?

¿Qué se debe definir?

La base de legitimación que permite el tratamiento, según la LOPDP.

Ejemplos comunes:

Ejecución de un contrato, Obligación legal, Interés legítimo, Consentimiento

¿Cómo se registra en el RAT?

"Consentimiento del titular para fines comerciales."
"Ejecución de contrato de prestación de servicios."

Actores en el Sistema de Protección de Datos Personales

¿Creamos un perfil con esos datos personales?

¿Qué se debe identificar?

Si se realiza perfilado para predecir comportamientos, preferencias o riesgos.

Ejemplos comunes:

Segmentación de clientes, evaluación crediticia, recomendaciones personalizadas.

¿Cómo se registra en el RAT?

"Si" o "No"

¿Enviamos esos datos a un tercero?

¿Qué se debe definir?

Si los datos se comunican o transfieren a otras entidades, dentro o fuera del país.

Ejemplos comunes:

Cumplir con un contrato, Atender solicitudes de servicio, etc.

¿Cómo se registra en el RAT?

"Sí."

"No se realiza ninguna transferencia."

Actores en el Sistema de Protección de Datos Personales

¿Requerimos de servicios de terceros para esta actividad?

¿Qué se debe identificar?

Si se utilizan encargados o sub-encargados para ejecutar parte del tratamiento.

Ejemplos comunes:

Segmentación de socios, evaluación crediticia, recomendaciones personalizadas.

¿Cómo se registra en el RAT?

"Sí, se utiliza un proveedor externo para almacenamiento en la nube (encargado)."

¿Qué medidas de seguridad se han implementado?

¿Qué se debe definir?

Las medidas técnicas, jurídicas, organizativas, administrativas y físicas que protegen los datos.

¿Cómo se registra en el RAT?

"Cifrado de datos, control de accesos, NDA firmados, backups semanales."

Transparencia hacia los Titulares

Datos de contacto de responsable y delegado

Derechos de los titulares

Datos personales objeto de tratamiento

Lenguaje sencillo, accesible y coherente

Canales para el ejercicio de derechos

Consentimiento libre, informado, específico, inequívoco.

Terceros y transferencias internacionales

Comunicación de incidentes de seguridad

Principales resoluciones emitidas por la Autoridad

No. Resolución	Nombre de Resolución
SPDP-SPDP-2024-0001-R	Estructura de la SPDP
SPDP-SPDP-2024-0002-R	Guía para el Registro de Apoderados Especiales
SPDP-SPDP-2024-0012-R	Guía para absolución de consultas
SPDP-SPDP-2024-0013-R	Reglamento para la Atención de Solicitudes y Denuncias
SPDP-SPDP-2024-0019-R	Lineamentos y directrices de la Política de Privacidad y Protección de Datos Personales
SPDP-SPDP-2024-0021-R	Reglamento para el procedimiento de suscripción, ejecución y seguimiento de convenios marco de cooperación interinstitucional
SPDP-SPD-2025-0003-R	Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales
SPDP-SPD-2025-0006-R	Reglamento que establece la obligación de incorporar cláusulas de protección de datos personales en los contratos celebrados dentro del territorio de la República del Ecuador

No. Resolución	Nombre de Resolución
SPDP-SPD-2025-0022-R	Reglamento para la aplicación de la metodología para el calculo de multas en el régimen administrativo sancionador de la SPDP
SPDP-SPD-2025-0024-R	Normativa general para la aplicación de La Ley Orgánica De Protección De Datos Personales y su reglamento en las Transferencias o Comunicaciones Nacionales e Internacionales de Datos Personales
SPDP-SPD-2025-0028-R	Reglamento del Delegado de Protección de Datos Personales (DPO)
SPDP-SPD-2025-0030-R	Reglamento para la seudonimización, anonimización, bloqueo y eliminación de datos personales
-	Guía de protección de datos desde el diseño y por defecto
SPDP-SPD-2025-0041-R	Normativa General para la aplicación del Interés Legítimo como Base de Legitimación para el Tratamiento de Datos Personales dentro del territorio de la República del Ecuador

Principales resoluciones emitidas por la Autoridad

Reglamento de cláusulas de protección de datos personales

Relaciones que requieren de una cláusula de protección de datos

Responsable - Titular

La COAC trata los datos personales de sus clientes para administrar su cuenta y evaluar operaciones financieras.

Responsable - Encargado

Un proveedor que trata datos personales de socios de la COAC para prestar el servicio de procesamiento transaccional, siguiendo las instrucciones de la COAC.

Responsable - Destinatario

La COAC transfiere los datos personales de sus socios a un TERCERO para finalidades propias de este último.

Responsables conjuntos

Dos entidades determinan conjuntamente las finalidades y tratamientos de datos personales para la gestión del producto financiero ofrecido.

Principales resoluciones emitidas por la Autoridad

Reglamento del Delegado de Protección de Datos Personales

Requisitos para el nombramiento del DPO

1. Fecha
2. Razón Social y RUC
3. Nombres del representante legal
4. Nombres y número de identificación del DPO
5. Referencia al cumplimiento de funciones
6. Firma autógrafa o electrónica del representante legal.
7. Aceptación del cargo (firma del DPO)

*El nombramiento deberá ser registrado **hasta quince (15) días después de haber sido otorgado digitalmente**. El incumplimiento a este plazo será considerado un incumplimiento de medidas de seguridad, sancionable como infracción grave.

Principales resoluciones emitidas por la Autoridad

Reglamento del Delegado de Protección de Datos Personales

El DPO deberá aprobar un programa de formación de los que sean formalizados por la SPDP.

Imparcialidad e independencia

El DPO podrá denunciar al responsable o encargado del tratamiento ante la SPDP por los hechos que pudieran menoscabar su independencia o que pudieran constituir una represalia en consideración de sus actuaciones.

Además, se deberán establecer mecanismos para la consideración efectiva de las observaciones y recomendaciones efectuadas por el DPO en relación con las actividades de tratamiento que se ejecuten; y, la consideración de los informes que determinen el nivel de cumplimiento de la normativa de protección de datos personales por parte de la COAC.

Las evaluaciones de cumplimiento de la organización deberán realizarse anualmente. En ningún caso la evaluación se podrá ejecutar por parte del DPO.

DGRV
Confederación Alemana de Cooperativas

Principales resoluciones emitidas por la Autoridad

Reglamento del Delegado de Protección de Datos Personales

Prohibiciones del DPO

Asumir funciones del responsable ni del encargado del tratamiento de datos personales.	Implementar directamente la normativa de protección de datos dentro de la organización.	Tomar decisiones sobre la finalidad o los medios del tratamiento de datos personales.	Gestionar riesgos o evaluaciones de impacto.
Desempeñar actividades que comprometan su independencia, autonomía o imparcialidad.	Representar a la organización ante la Superintendencia de Protección de Datos Personales.	Ocupar cargos como oficial de seguridad, de cumplimiento o implementador, u otros que generen conflicto de interés.	Ejercer funciones que afecten su independencia, imparcialidad u objetividad.

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

DGRV
Confederación Alemana de Cooperativas

Principales resoluciones emitidas por la Autoridad

Reglamento del Delegado de Protección de Datos Personales

¿Cuándo existe conflicto de interés?

01 02 03

1. El delegado designado ejecutare una o varias actividades de tratamiento de datos personales, o si participare en el desarrollo de su ejecución de forma ocasional o permanente.

2. El delegado ejerciere acciones de asesoría que, ajenas a sus funciones como delegado, tuvieren por objetivo salvaguardar los intereses de la organización

3. El delegado tomare decisiones sobre la organización, sus actividades o sus gestiones internas.

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

Principales resoluciones emitidas por la Autoridad

Normativa General para la aplicación del Interés Legítimo

Características del interés legítimo

1. Lícito
2. Real y concreto
3. Proporcional
4. Compatible con las expectativas razonables del titular

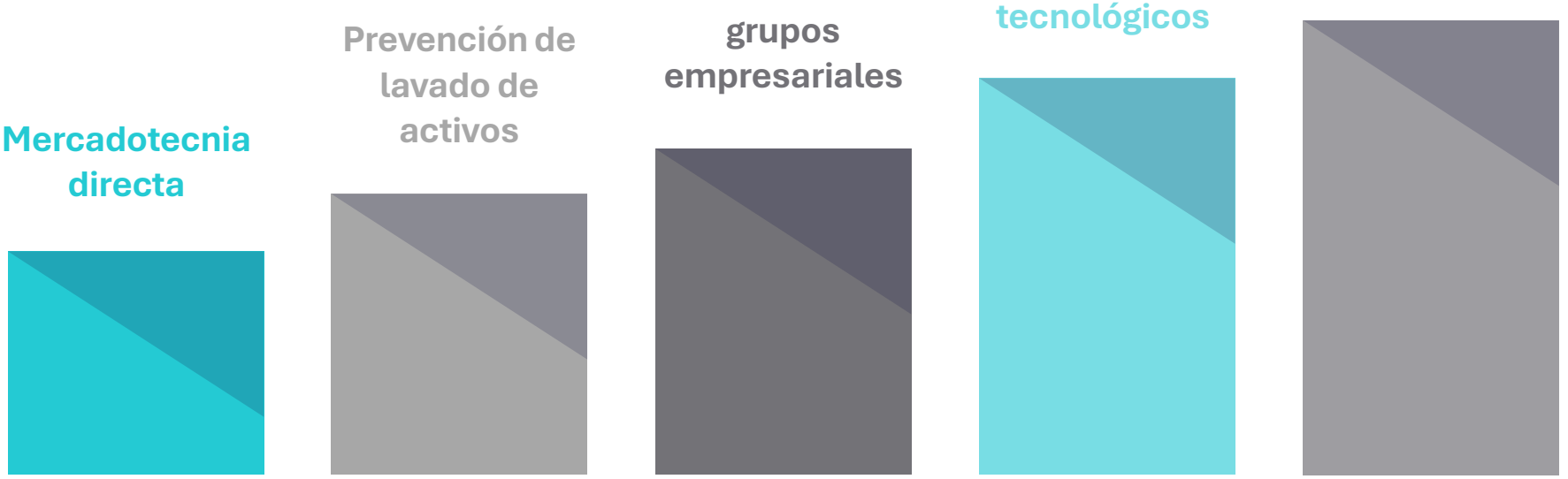
Evaluación de ponderación

Determina si el interés invocado por el responsable del tratamiento prevalece frente a los derechos y libertades de los titulares.

Principales resoluciones emitidas por la Autoridad

Normativa General para la aplicación del Interés Legítimo

¿En qué casos se puede invocar un interés legítimo como base de legitimación?



Absoluciones de consulta relevantes

Datos biométricos para registro de asistencia

El tratamiento de datos biométricos cabe cuando se cumplen 4 requisitos: prueba de proporcionalidad; análisis de riesgo; evaluación de impacto; y, consentimiento del colaborador.

El consentimiento será válido cuando el colaborador cuente con varias opciones de registro y él escoja voluntariamente el uso de datos biométricos.

Designación de DPO por parte de COAC

La absolución de consulta determinó que las Cooperativas de Ahorro y Crédito están obligadas a designar un DPO debido que hacen un **tratamiento a gran escala de datos crediticios**. Esta designación es obligatoria desde que entraron en vigor la LOPDP y su Reglamento.

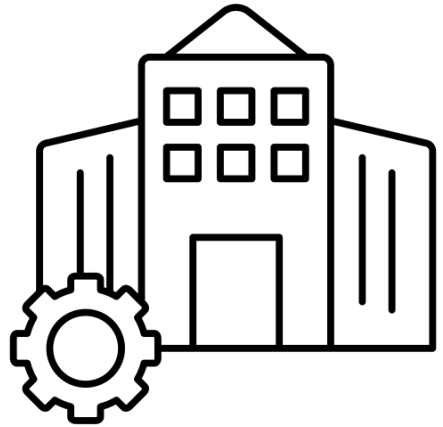
Aceptación de Política de Protección de Datos

Cuando el tratamiento de datos personales se basa en una base legal distinta del consentimiento, los responsables pueden proceder con el tratamiento sin obtener la aceptación expresa de la política de protección de datos por parte del titular. La Autoridad enfatizó que, si bien la adopción de dicha política es una obligación, su validez no está condicionada al consentimiento del titular.

Principales resoluciones emitidas por la SEPS

Norma de buen gobierno cooperativo para el sector financiero popular y solidario

Resolución No. SEPS-IGT-IGS-IGJ-INR-INSESF-INFMR-INGINT-2025-0144



¿Qué deben considerar las COAC al implementar un programa de buen gobierno corporativo?

Principio de Transparencia

Actuar de manera clara y honesta permitiendo el acceso a la información asegurando la transparencia en los procesos de toma de decisiones.

Política de revelación y tratamiento de información

Tomar en cuenta los principios, derechos y disposiciones establecidas en la Ley Orgánica de Protección de Datos Personales.

Principales resoluciones emitidas por la SEPS

Norma de control para la calificación y supervisión de las compañías de servicios auxiliares

Los contratos entre compañías de servicios auxiliares y COAC deben contener una cláusula de protección de datos personales. Por ende, estas deben cumplir con los mínimos establecidos por la SPDP en la resolución No. SPDP-SPD-2025-0006-R.

Resolución No. SEPS-IGT-IGS-IGJ-INR-INSESF-INSEPS-INGINT-2025-0147

Norma de canales electrónicos

Las COAC deberán implementar:

- Medidas de seguridad de la información.
- Medidas de seguridad tecnológicas.
- Planes de mitigación ante un incidente de seguridad.
- Métodos de validación de identidad del socio en canales electrónicos.
- Procedimientos para atender reclamos del socio (por ejemplo, procedimientos ante una solicitud de ejercicio de derechos).
- Procedimientos de auditoría de seguridad en canales electrónicos una vez al año.

Resolución No. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009

DGRV
Confederación Alemana de Cooperativas

Casos emblemáticos

50 AÑOS CORRAL ROSALES

CAMBRIDGE ANALYTICA

Cambridge Analytica, con una multa de USD **68 millones** la sociedad de análisis que explotó en su propio beneficio los datos de casi **90 millones de usuarios de Facebook**, al que acusaron de negligencia.

BRITISH AIRWAYS

Una multa de USD **26 millones**. Los sistemas de British Airways se vieron comprometidos. La brecha afectó a 400.000 clientes se obtuvieron los datos de inicio de sesión, la información de la tarjeta de pago y los nombres y direcciones.

AMAZON

La multa gigantesca de GDPR de Amazon, (USD **877 millones**), anunciada en el informe de ganancias de julio de 2021 de la compañía, es casi 15 veces mayor que el récord anterior, la causa tiene que ver con el consentimiento de las cookies.

GOOGLE

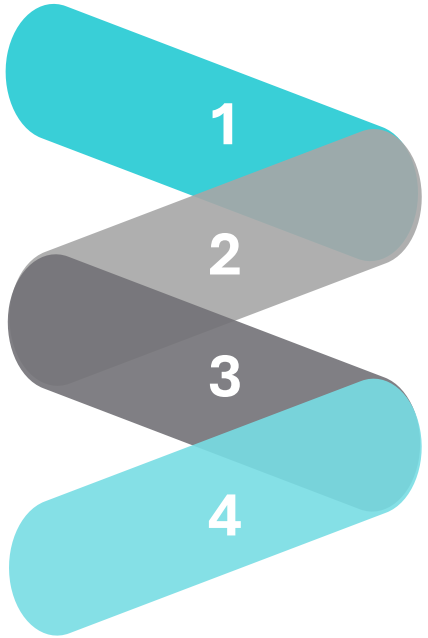
La autoridad francesa de protección de datos golpeó a Google Irlanda con una multa de **USD 102 millones**, por la forma de implementar los procedimientos de consentimiento de cookies.

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

Casos prácticos – Ejercicio de derechos

1 Un socio proporcionó sus datos en un formulario online de solicitud de préstamo de la COAC Fuerza Ecuador, que le otorgó un préstamo de 300 dólares.

2 Al demorar en el pago, la deuda fue transferida a la empresa de cobranza "Yo Cobro", la cual gestionó los cobros mediante correos electrónicos, acusando al socio de moroso y adjuntando documentación sobre la deuda.



3 "Yo Cobro" utilizó tanto el correo electrónico personal como el de trabajo del socio, este último **no fue** proporcionado por él.

4 El socio presenta un reclamo en contra de la Cooperativa y "Yo Cobro". En respuesta, la Cooperativa manifiesta que la empresa de cobranza actuó sin su intervención ni supervisión.

Potenciales repercusiones

i. "Yo Cobro" realizó un **tratamiento ilícito** y no autorizado de datos personales al utilizar el correo profesional del titular, el cual no fue facilitado.

ii. "Yo Cobro" incurrió en una infracción grave establecida en el artículo 70 numeral 1 de la LOPDP, pues se **vulneró el principio de confidencialidad**.

iii. La SPDP podría imponer una multa de entre el **0,7% al 1%** del volumen de negocio de "Yo Cobro".

Casos prácticos – Vulneraciones de seguridad

El **17 de noviembre de 2025**, uno de los miembros del personal de la COAC “ABC” recibió un correo a su bandeja de mensajes no deseados de su cuenta de correo corporativo.

En este mensaje se le notificó el bloqueo de su tarjeta de ingreso a las instalaciones de forma temporal. Sin embargo, en el correo se da la opción de volver a activar la tarjeta haciendo click en el botón “Activar”.

Pese a que ABC cuenta con medidas de seguridad técnicas, la persona quien dio click en el botón “Activar” tiene una contraseña débil para iniciar sesión en los programas informáticos de la COAC. Esto le ha permitido a un hacker acceder a bases de datos de socios de ABC.

La base de datos de socios y proveedores a la que ha accedido el hacker tiene la siguiente información: razón social, RUC, dirección, números de teléfono, y tipo de actividad económica. Es decir, datos que ayudan a la gestión de facturación y emisión de comprobantes de retención.

¿Cómo se debería actuar?

Quito

Robles E4-136 y Av. Amazonas Edif. Proinco Calisto, piso 12

T.: +593 2 2544144

Guayaquil

Av. Francisco de Orellana 234 Edif. Blue Tower, piso 6

T.: +593 2 630441

50 AÑOS CORRAL ROSALES

DGRV

Confederación Alemana de Cooperativas

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA