

¿Cómo ARGBroker debe implementar seguridad según la Ley de Protección de Datos Personales. ?

En Argentina, la ley de protección de datos personales se rige principalmente por la Ley Nacional de Protección de Datos Personales (Ley 25.326) y su reglamento.

1. **Designación de un Encargado de Protección de Datos (DPO):** ARGBroker debe designar un Encargado de Protección de Datos (DPO) o Responsable de Protección de Datos, cuya función principal es garantizar el cumplimiento de la ley de protección de datos dentro de la organización.
2. **Consentimiento informado:** ARGBroker debe obtener el consentimiento informado de los individuos para recopilar, procesar y almacenar sus datos personales. Este consentimiento debe ser específico, inequívoco y otorgado libremente por la persona.
3. **Seguridad de los datos:** La empresa debe implementar medidas de seguridad técnicas y organizativas adecuadas para proteger los datos personales contra el acceso no autorizado, la divulgación, la alteración o la destrucción. Esto puede incluir la encriptación de datos, el control de acceso, la pseudonimización, entre otras medidas.
4. **Análisis de riesgos y evaluación de impacto:** ARGBroker debe realizar análisis de riesgos y evaluaciones de impacto de forma periódica para identificar posibles vulnerabilidades en el tratamiento de datos personales y tomar medidas para mitigar esos riesgos.
5. **Notificación de brechas de seguridad:** En caso de que ocurra una violación de seguridad que afecte los datos personales, ARGBroker está obligado a notificar la brecha a la Agencia de Acceso a la Información Pública (AAIP) y a los individuos afectados en los términos establecidos por la ley.
6. **Transferencia internacional de datos:** Si ARGBroker planea transferir datos personales fuera de Argentina, debe asegurarse de que existan garantías adecuadas para proteger la privacidad y seguridad de esos datos, ya sea a través de la obtención de autorización de la AAIP o utilizando mecanismos de transferencia reconocidos por la ley.
7. **Formación del personal:** La empresa debe proporcionar formación adecuada sobre seguridad de datos y cumplimiento de la ley de protección de datos a su personal que maneje datos personales.
8. **Registro de bases de datos:** ARGBroker debe mantener un registro de las bases de datos que contienen datos personales, que incluya información sobre la finalidad del tratamiento, las medidas de seguridad implementadas, entre otros detalles.

¿Si el cliente decide reemplazar a ARGBroker por otro proveedor, describir cómo se debe actuar de manera ética ante el cliente y los colegas ?

Cuando un cliente decide reemplazar a ARGBroker por otro proveedor, es importante actuar de manera ética y profesional tanto hacia el cliente como hacia los colegas.

1. **Transparencia y comunicación abierta con el cliente:** Es fundamental ser transparente con el cliente y comunicar claramente los motivos del cambio de proveedor, así como cualquier impacto que pueda tener en el servicio o en la relación comercial. Proporcionar información honesta y completa ayudará a mantener la confianza del cliente.
2. **Facilitar una transición suave:** ARGBroker debe esforzarse por garantizar una transición suave y sin problemas para el cliente hacia el nuevo proveedor. Esto puede implicar

proporcionar documentación relevante, asistencia técnica durante el proceso de migración y garantizar la transferencia ordenada de datos y activos.

3. **Respetar la confidencialidad y la privacidad del cliente:** Durante el proceso de transición, es importante respetar la confidencialidad y la privacidad de la información del cliente. Esto significa no divulgar información confidencial a terceros sin el consentimiento del cliente y garantizar que los datos sean transferidos de manera segura y conforme a las leyes y regulaciones aplicables.
4. **Mantener la profesionalidad con los colegas:** Es crucial mantener la profesionalidad y el respeto hacia los colegas durante todo el proceso. Evitar comentarios negativos o despectivos sobre el cliente o el nuevo proveedor, y centrarse en trabajar en colaboración para garantizar una transición exitosa.
5. **Aprender de la experiencia:** Después de que se complete la transición, es importante reflexionar sobre la experiencia y buscar oportunidades de aprendizaje. Identificar áreas en las que ARGBroker podría haber mejorado su servicio o relación con el cliente ayudará a la empresa a crecer y mejorar en el futuro.

[¿Si un usuario denuncia a ARGBroker por divulgación de sus datos personales, a que legislación recurrió el mismo y como ARGBroker puede respaldarse jurídicamente.?](#)

En Argentina, si un usuario denuncia a ARGBroker por divulgación de sus datos personales, la legislación a la que probablemente recurra el usuario es la Ley Nacional de Protección de Datos Personales (Ley 25.326) y su reglamentación, así como también la Ley de Defensa al Consumidor (Ley 24.240).

Para respaldarse jurídicamente, ARGBroker debe demostrar que ha cumplido con todas las disposiciones de la Ley de Protección de Datos Personales y cualquier otra legislación aplicable. Aquí hay algunas formas en las que ARGBroker puede respaldarse en Argentina:

1. **Consentimiento informado:** ARGBroker debe demostrar que obtuvo el consentimiento informado del usuario para el tratamiento de sus datos personales, de acuerdo con lo establecido en la Ley 25.326. Esto implica tener registros de consentimiento que muestren que el usuario fue informado sobre cómo se utilizarían sus datos y otorgó su consentimiento de manera libre, específica e inequívoca.
2. **Política de privacidad y seguridad de datos:** ARGBroker debe tener una política de privacidad clara y accesible que explique cómo se recopilan, almacenan, utilizan y protegen los datos personales de los usuarios. La política debe cumplir con los requisitos establecidos por la Ley 25.326 y reflejar las mejores prácticas en materia de seguridad de datos.
3. **Medidas de seguridad de datos:** La empresa debe demostrar que ha implementado medidas de seguridad técnicas y organizativas adecuadas para proteger los datos personales de los usuarios contra accesos no autorizados, divulgación, alteración o destrucción, tal como lo exige la Ley 25.326 y su reglamentación.
4. **Registro de bases de datos:** ARGBroker debe mantener un registro de las bases de datos que contiene datos personales, de acuerdo con lo establecido en el artículo 21 de la Ley 25.326. Este registro debe incluir información sobre la finalidad del tratamiento, las medidas de seguridad implementadas y otros detalles requeridos por la ley.
5. **Notificación de brechas de seguridad:** Si se produce una brecha de seguridad que afecta los datos personales de los usuarios, ARGBroker debe demostrar que cumplió con su

obligación de notificar la brecha a la Agencia de Acceso a la Información Pública (AAIP) y a los usuarios afectados, según lo establecido en la Ley 25.326.

Al respaldarse jurídicamente de esta manera, ARGBroker puede demostrar que ha cumplido con sus obligaciones legales en materia de protección de datos personales y defenderse de las acusaciones de divulgación indebida de datos en Argentina. Es importante que la empresa consulte con asesores legales especializados para garantizar el cumplimiento completo de la legislación aplicable y tomar las medidas adecuadas en caso de denuncia por parte de un usuario.