Assessing the risk of a data breach in 5 steps

The level of risk generated by a personal data breach must be assessed on a case-by-case basis.

It will depend in particular on the following criteria:

- the nature of the data (sensitive, biometric, financial, etc.);
- the number and categories of the affected individuals, particularly if they are vulnerable (people with disabilities, minors, employees, etc.);
- how easy it is to identify the affected individuals following the breach;
- existing security measures (encryption, pseudonymization, restricted access, etc.);
- the ability to detect and react rapidly to the incident.

To assess the risk level of a data breach, the APDP suggests that you follow the 5 steps below:

1. Verification of the need to assess risk

- Does the incident involve **personal data**?
- Is there a **potential impact on the rights and freedoms** for the affected individuals?

If the answer to these two questions is **yes, a risk assessment is mandatory**.

2. Assessing the severity of the consequences for the affected individuals

This step measures the **possible** impact on affected individuals:

LEVEL	POSSIBLE CONSEQUENCES
Low	Minor inconvenience, little impacts on private life.
Medium	Real but limited risk: minor financial loss, discrimination.
High	Serious or irreversible damage: reputation, health, identity theft.

3. Assessing the likelihood of damage occurring

This step estimates the **probability of damage occurring:**

LEVEL	INDICATORS
Low	Protected data, limited access, isolated incident. Effective corrective measures.
Medium	Partial, imperfect defences. Plausible risk of the incident recurring if no preventive action is taken.
High	Data exposed, known vulnerability. The incident is likely to recur almost immediately if no corrective/technical action is taken as soon as possible.

4. Identification of the level of risk using a cross matrix (severity × likelihood)

Once the likelihood and severity have been assessed, these elements can be entered in the following matrix (the vertical axis representing severity and the horizontal axis likelihood):

		LIKELIHOOD		
		Low	Medium	High
SEVERITY	Low	Low risk	Medium risk*	Medium risk
	Medium	Medium risk*	Medium risk	High risk
	High	Medium risk	High risk	High risk

*Medium risk that can be reduced to low risk if appropriate preventive measures are taken.

5. Consequences of the assessment

Now that the risk has been identified, the data controller can take technical and organisational measures to limit the impact of the breach and prevent it from happening again.

[For more information, refer to the factsheet **The main data breaches: obligations and advice on how to prevent them]**

In addition, under article 32 of Law no. 1.565 of December 3, 2024, the data controller must notify the APDP of any data breach **likely** to pose a **risk to the rights and freedoms** of the affected individuals.

Depending on the level of seriousness, it may also be necessary to **inform the affected individuals**.

Level of risk	Mandatory action(s)
No risk	- Entry in the data breach register
Low risk	- Entry in the data breach register - Notification to the APDP within 72 hours
Medium risk	- Entry in the data breach register - Notification to the APDP within 72 hours
High risk	- Entry in the data breach register - Notification to the APDP within 72 hours - Communication to the affected individuals

[For more information, refer to the factsheet **Notification of personal data breaches**]