

Telefónica

Data Security

The challenge of protecting data in a connected business

The more connected an organisation is, the more difficult it is to maintain control over its data.

Data is one of the **most important assets of any organisation**, but also one of the most difficult to protect when it is spread across different environments, users, and tools.

Sensitive information is spread across **data centres, the cloud, SaaS applications, workstations, and artificial intelligence tools.** In order to protect it, you need to know which information is sensitive, where it is located, what risks it faces, and how it is used. The aim is to reduce risk without holding back the business.

A comprehensive view of data security

Do you know where your sensitive data is and what risks it faces?

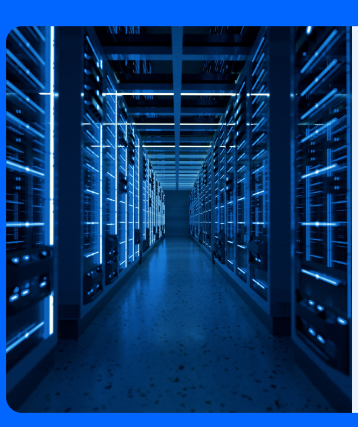
Protecting data involves much more than just knowing where it is. It also means identifying it, understanding the risks, safeguarding it against misuse and maintaining control over it.



Data Security Posture Management (DSPM)

Understand your data and prioritise risks

Discover and classify sensitive information, assess its security across cloud environments and identify exposure risks, excessive permissions and insecure configurations to prioritise its protection.



Data Loss Prevention (DLP)

Prevent data leaks without slowing down business

Detect and control the outflow or misuse of sensitive information in email, on the web, in the cloud, on endpoints, and in AI tools. Add context to identify potential internal threats and reduce data leaks.



Information Rights Management (IRM)

Keep control over who accesses and uses your documents

Control sensitive documents through encryption, granular permissions, traceability, and revocation. Protection remains in place even if the file is shared or leaves the organisation.

Two capabilities to integrate data security into strategy and operations



Data Security Consultancy

Determine how to protect your data

Assess the current situation, identify critical data and risks, and define priorities and a roadmap. This includes governance, classification, policies, architecture, and support in selecting solutions.



Managed Services for Data Security

Manage data security on an ongoing basis

Deploy, integrate, and operate data security capabilities. This includes policy tuning, alert analysis, internal threat investigation, incident support, reporting, and continuous improvement.

What benefits does it bring to your organisation?

Greater visibility

Understand your sensitive data and its exposure to prioritise risks.

Reduced risk of data breaches

Detect and anticipate the misuse of sensitive information.

Persistent control

Maintain document protection both within and outside the organisation.

More context for action

Correlate data, users and activity to investigate anomalous behaviour.

Why Telefónica?

We are the best route for businesses and institutions to access digital technologies.

We bring together cybersecurity specialists, data protection and management capabilities, and managed services to help you identify where your sensitive data is located, understand how it is used, prioritise risks and protect information against unauthorised access, wherever it resides.