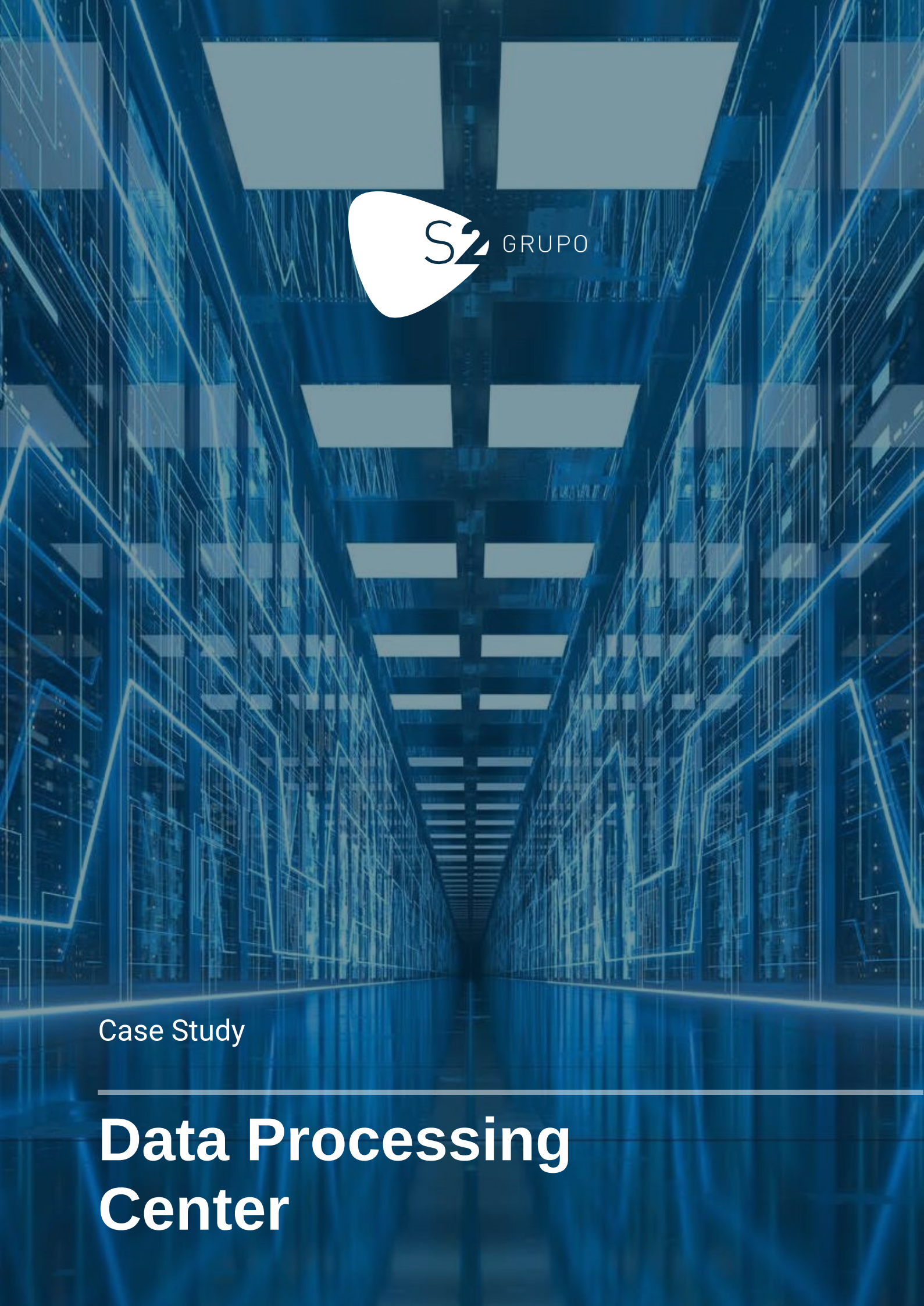

Case Study

Data Processing Center

Brief presentation of the company:

It is an important financial entity with a **data processing center** from where business activity, transactions and movements are controlled permanently 24 hours a day.

The operation of the data center is essential for the company's activity. It has all its services redundantly duplicated to ensure business continuity on a permanent basis.

In addition to the infrastructure for information management, the data center needs other fundamental complementary facilities: a power supply with no outages or interruptions, temperature and humidity conditions that allow the proper operation of all the network electronics and the large amount of heat generated by this equipment. Fire protection installations with automatic fire detection and extinguishing, access control, security lighting, etc.

Description of the problem/challenge

The company already has personnel specialized in ensuring IT cybersecurity conditions for the security of its customers' information.

But it has no experience or expertise in operational cybersecurity - that which can affect the operation of the facilities required to maintain the data center.

A problem in the power supply, cooling or protection installations would affect the operation of an infrastructure essential to the company's business continuity.

You need to know the level of risk in the facilities that keep the data center in service.

2. Description of the work performed

A team of experts in industrial cybersecurity travels to the DPC to analyze the related installations, their distribution and critical elements for operation.

The management of the electricity, air conditioning and security installations is supervised from a centralized management system with interconnections with the different equipment and both local and remote access.

A series of pre-planned tests of limited scope with a low degree of intrusion are carried out, which in no case can affect the operation of the DPC. It is verified that it is possible to remotely access critical elements of the facilities. In this way, it is shown that it would be possible to accidentally or intentionally manipulate the operation of the facilities that keep the data center in service.

As a result of the analysis and tests carried out, a report is prepared detailing the checks performed, the results obtained and the measures recommended to mitigate the potential risks detected.

3. Benefits Obtained

With the realization of this project, the client:

1

May check the degree of vulnerability of a business-critical asset by uncovering potential risks that were not previously considered.

2

This assessment gives you a complete picture of the operational cybersecurity status of your critical facilities. Based on the results obtained, you know the risks and can take measures to avoid an incident that could jeopardize the continuity of your business.

3

Allows you to draw up an action plan that limits risks and avoids service interruption of your infrastructures.

S2 GRUPO

Anticipando un mundo
ciberseguro

MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLA
SAN SEBASTIÁN

SANTIAGO DE CHILE
C.D. MÉXICO
BOGOTÁ
BRUSELAS
LISBOA
RÓTERDAM

Síguenos • **@s2grup** • **s2grupo.e**