S2 GRUPO
Anticipating a
cyber secure world

CASE STUDY

Incident response **Training**

01

Introduction

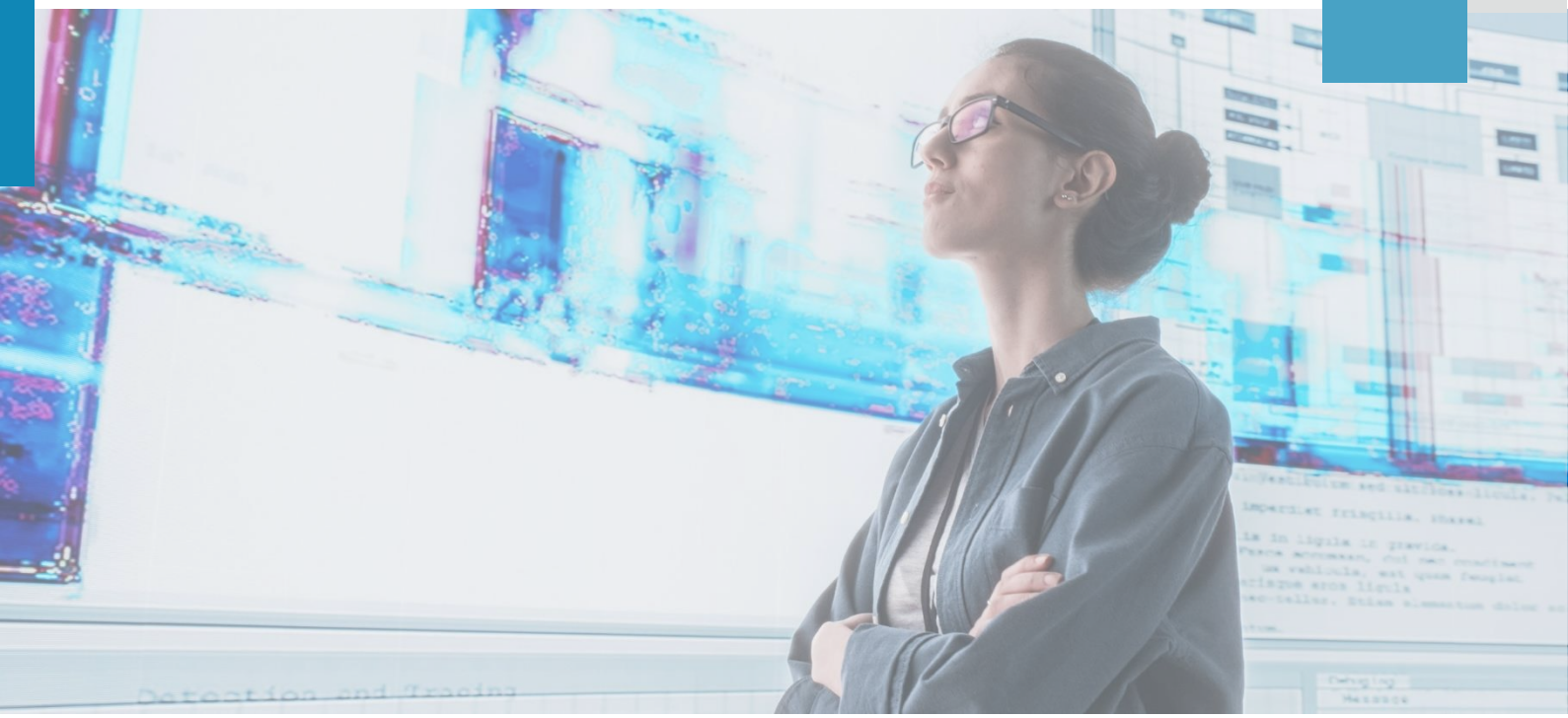
It is one of the largest consumer goods companies in Peru, although it also has offices in the rest of Latin America. The company has different business lines and more than 150 own brands.

The company has a **cybersecurity team led by the CISO**. Until now, its functions have been mainly focused on cybersecurity in the IT area.

They have a document system related to cybersecurity, mainly focused on the Incident Response Plan. Associated with it, they have several IT playbooks.

02

Problem/challenge



The company has previously conducted exercises and workshops to train all employees in the process of dealing with a potential cybersecurity incident.

It needs to conduct exercises at the technical and executive level that represent a simulated cyber incident that could happen exactly the same way in reality. In addition, all the information used to conduct the exercises must be able to occur in the same way in a real case.

The exercises are presented in a mixed format (one group of people attending remotely and another group of people attending in person), so the session must be adapted to both formats.

03

Upgrade performed

All the documents related to incident response (incident response plan and playbooks) are analyzed in order to organize workshops prior to the drill for the team of technicians and executives. The aim of these workshops is to ensure that all employees are aware of the contents of each document and their roles and responsibilities in the event of an incident. At the end of these workshops, all employees should be able to respond appropriately to a cybersecurity incident.

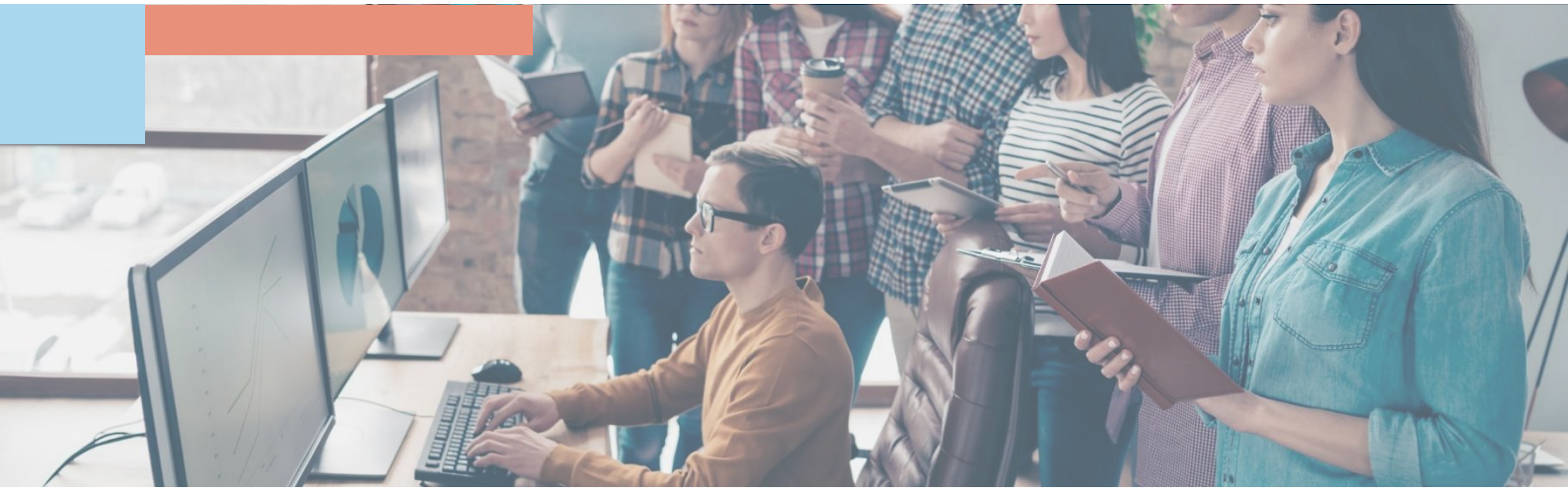
To carry out these workshops, 3 people from S2 Grupo's industrial safety team travel to the client's facilities in Peru..

After the workshops, three simulation exercises are planned to be carried out.

The main objective of the simulation exercises is to test the company's preparedness and capacity to face and manage cybersecurity incidents, evaluating the effectiveness of the procedures, policies and resources available in the detection, analysis, containment and recovery of incidents, as well as strategic decision making.

A simulation exercise is designed based on a possible real case. To this end, meetings are held with various departments within the client (communication, risk, operations, distribution, etc.) in order to obtain all the necessary information to model the exercise as close to reality as possible.

Three separate exercises are convened (two of them aimed at technicians and one aimed at executives). The objective is for the incident to be detected by the team of technicians in the first session, to continue working on it in the second session, and to report it to the executive team (Crisis Committee) in the third session.



For this purpose, the case is focused on a ransomware infection, including all phases of the process.

The dynamics of the exercises is the same for all sessions. Different scenarios are presented in chronological order and attendees must make decisions based on injectors and following the company's incident response plan. The injectors are new information entering the process that requires action by the incident response team.

To carry out these exercises, 3 people from S2 Grupo's industrial cybersecurity team travel to the client's facilities in Peru.

Since all the sessions are given by these 3 people, one of them is assigned to attend to the personnel attending the session remotely.

As a result of the exercises, an executive report is prepared including a general description of the exercises, the list of participants, the lessons learned during the exercises detailing the strengths and weaknesses encountered, as well as recommendations for future exercises.

04

Benefits obtained

With the completion of this project the client:

- Ensured in a didactic manner that all employees were aware of the company's incident response plan and associated playbooks.
- Didactically verified that all workers were aware of their roles and functions within the incident response plan.
- Reviewed that both the incident response plan and associated playbooks were up to date.

S2 GRUPO

MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLE
SAN SEBASTIAN

SANTIAGO DE CHILE
C.D. MEXICO
BOGOTA
LISBON
ROTERDAM

Follow us: @s2grupo • s2grupo.es