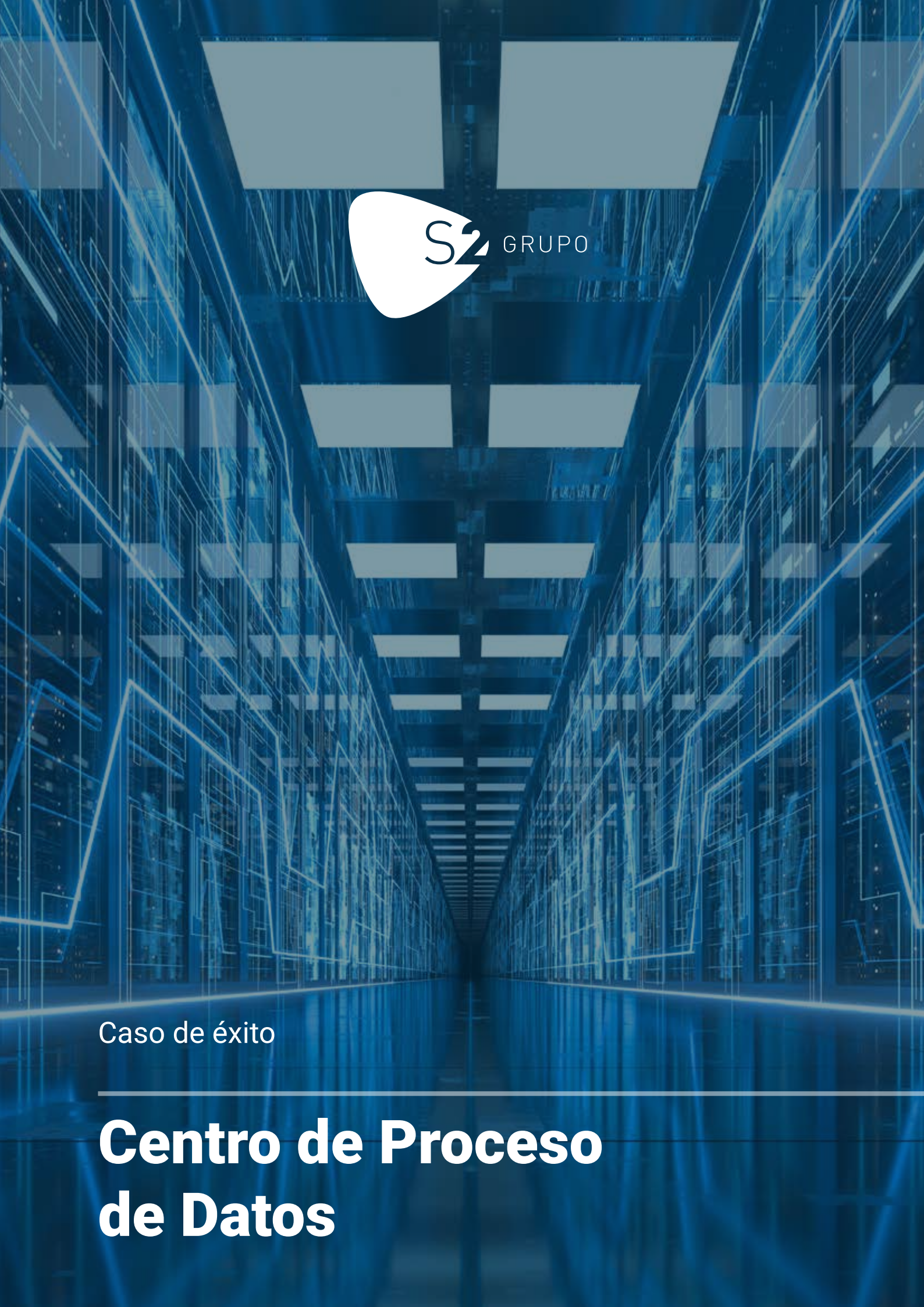
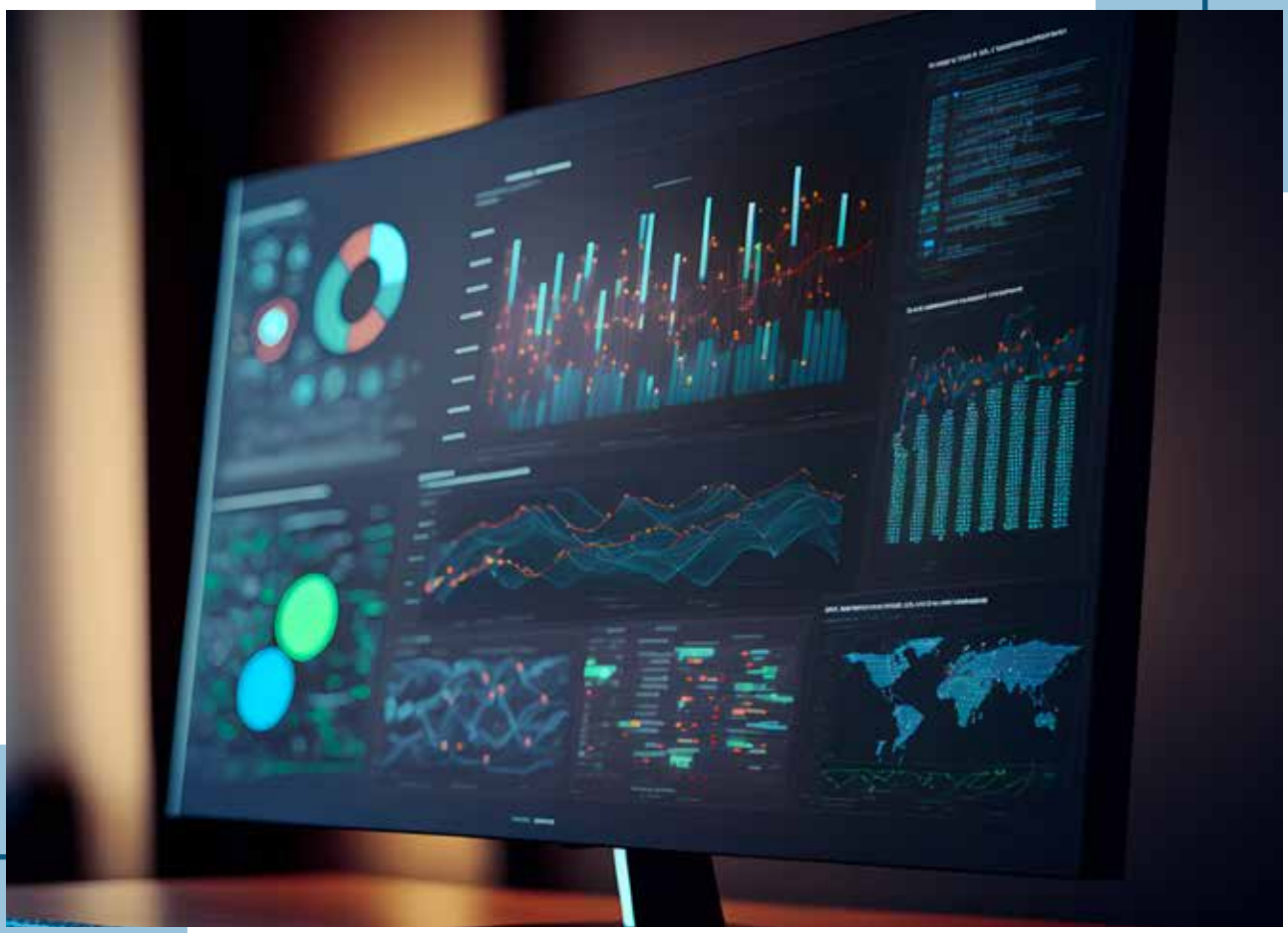


Caso de éxito

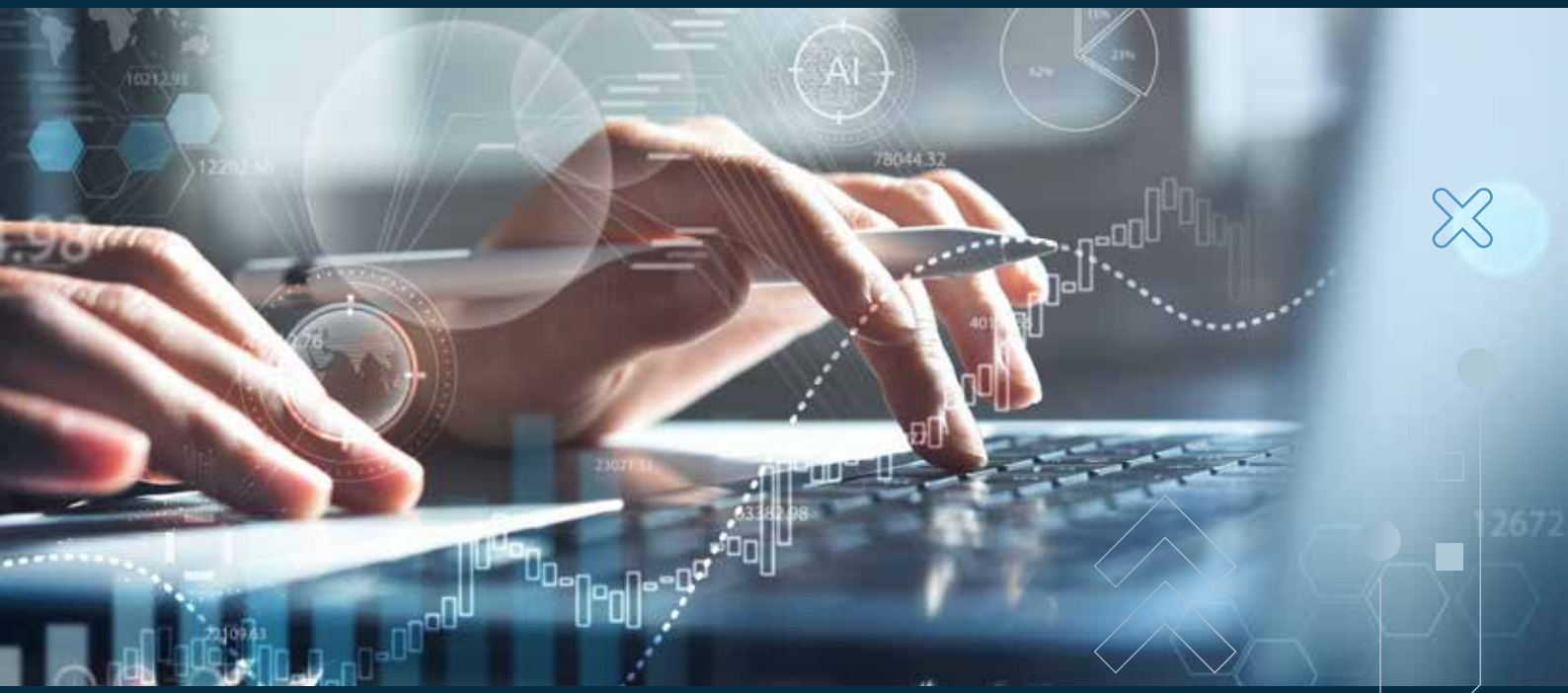
Centro de Proceso de Datos

Breve presentación de la empresa:

Se trata de una importante entidad financiera con un **centro de proceso de datos** desde dónde se controla la actividad del negocio, transacciones y movimientos de forma permanente 24 horas al día.



El funcionamiento del centro de datos es esencial para la actividad de la empresa. Cuenta con todos sus servicios duplicados de forma redundante para garantizar la continuidad del negocio de forma permanente.



Además de la infraestructura para la gestión de la información el centro de datos necesita otras instalaciones complementarias fundamentales: suministro de energía eléctrica sin cortes ni interrupciones, unas condiciones de temperatura y humedad que permitan el funcionamiento adecuado de toda la electrónica de red y la gran cantidad de calor que estos equipos generan. Unas instalaciones de protección de incendios con detección y extinción automática, control de accesos, alumbrado de seguridad, etc.

1. Descripción de la problemática/reto

La compañía ya dispone de personal especializado en garantizar unas condiciones de ciberseguridad IT en lo relacionado con la seguridad de la información de sus clientes.

Pero no dispone de experiencia ni conocimientos en los relacionado con la ciberseguridad operacional: aquella que puede afectar al funcionamiento de las instalaciones necesarias para el mantenimiento del CPD.

Un problema en el suministro de energía, en la refrigeración o en las instalaciones de protección afectaría al funcionamiento de una infraestructura esencial para la continuidad del negocio de la compañía.

Necesita conocer el nivel de riesgo en las instalaciones que mantienen el centro de datos en servicio.

2. Descripción de la actuación realizada

Un equipo de expertos en ciberseguridad industrial se desplaza al CPD para analizar las instalaciones relacionadas, su distribución y sus elementos críticos para el funcionamiento.

La gestión de las instalaciones de electricidad, climatización y seguridad se supervisa desde un sistema de gestión centralizada con interconexiones con los diferentes equipos y acceso tanto local como remoto.

Se realiza una serie de pruebas previamente planificadas y de alcance limitado con un bajo grado de intrusión que en ningún caso puedan llegar a afectar al funcionamiento del CPD. Se comprueba que es posible acceder de forma remota a elementos críticos de las instalaciones. De este modo se evidencia que sería posible manipular de forma accidental o intencionada el funcionamiento de las instalaciones que mantienen en servicio el centro de datos.

Como resultado del análisis y de las pruebas efectuadas se elabora un informe que detalla las comprobaciones realizadas, los resultados obtenidos y las medidas recomendadas para mitigar los riesgos potenciales detectados.

3. Beneficios Obtenidos

Con la realización de este proyecto el cliente:

1

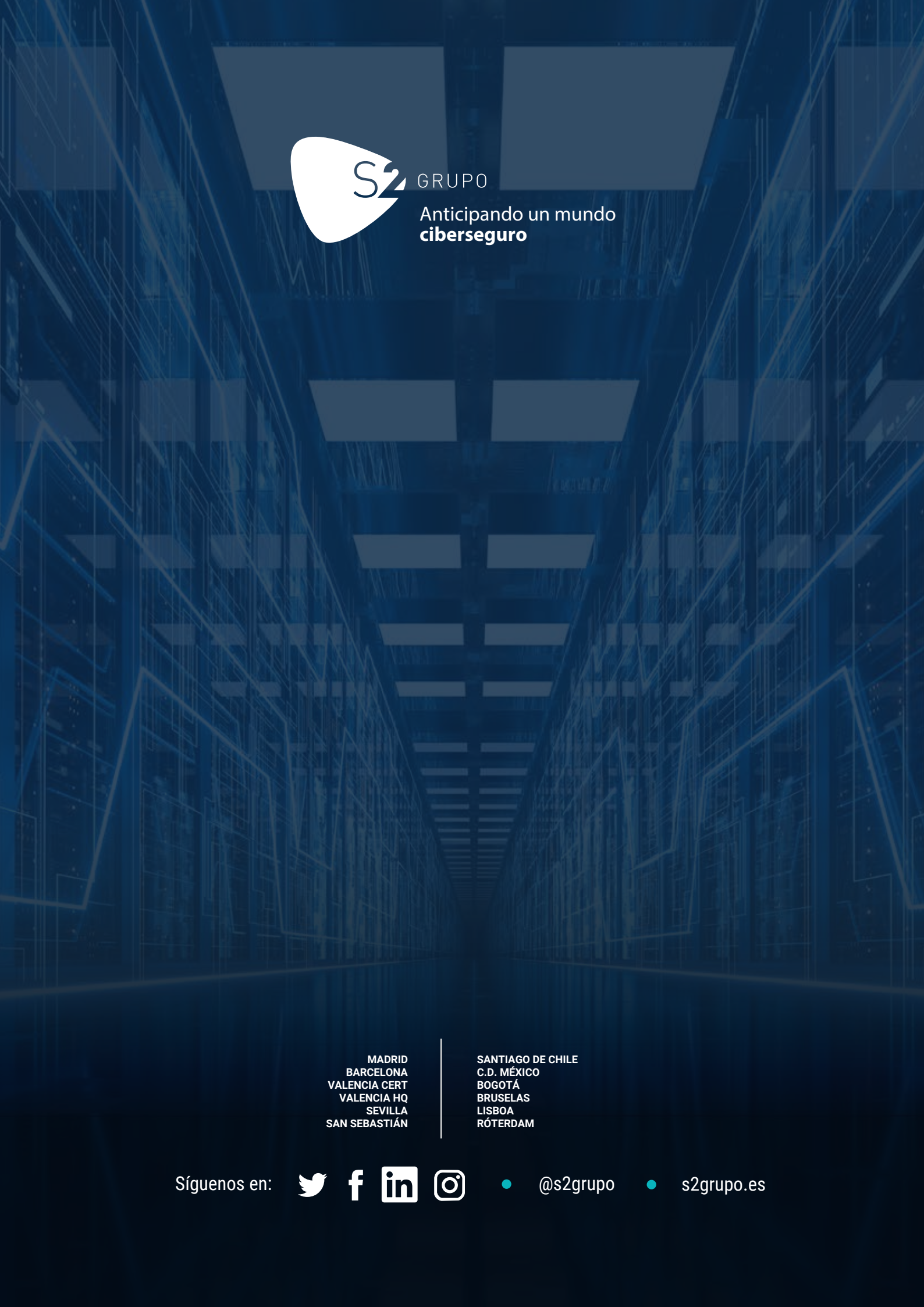
Comprueba el grado de vulnerabilidad de un activo crítico para su negocio descubriendo riesgos potenciales que no habían sido tenidos en cuenta.

2

Esta evaluación le permite disponer de una visión completa del estado de la ciberseguridad operacional de sus instalaciones esenciales. En función de los resultados obtenidos conoce los riesgos y puede adoptar medidas para evitar un incidente que pondría en riesgo la continuidad de su actividad.

3

Le permite confeccionar un plan de acción que limite los riesgos y evite la interrupción del servicio de sus infraestructuras.



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 en: • @s2grupo • s2grupo.es