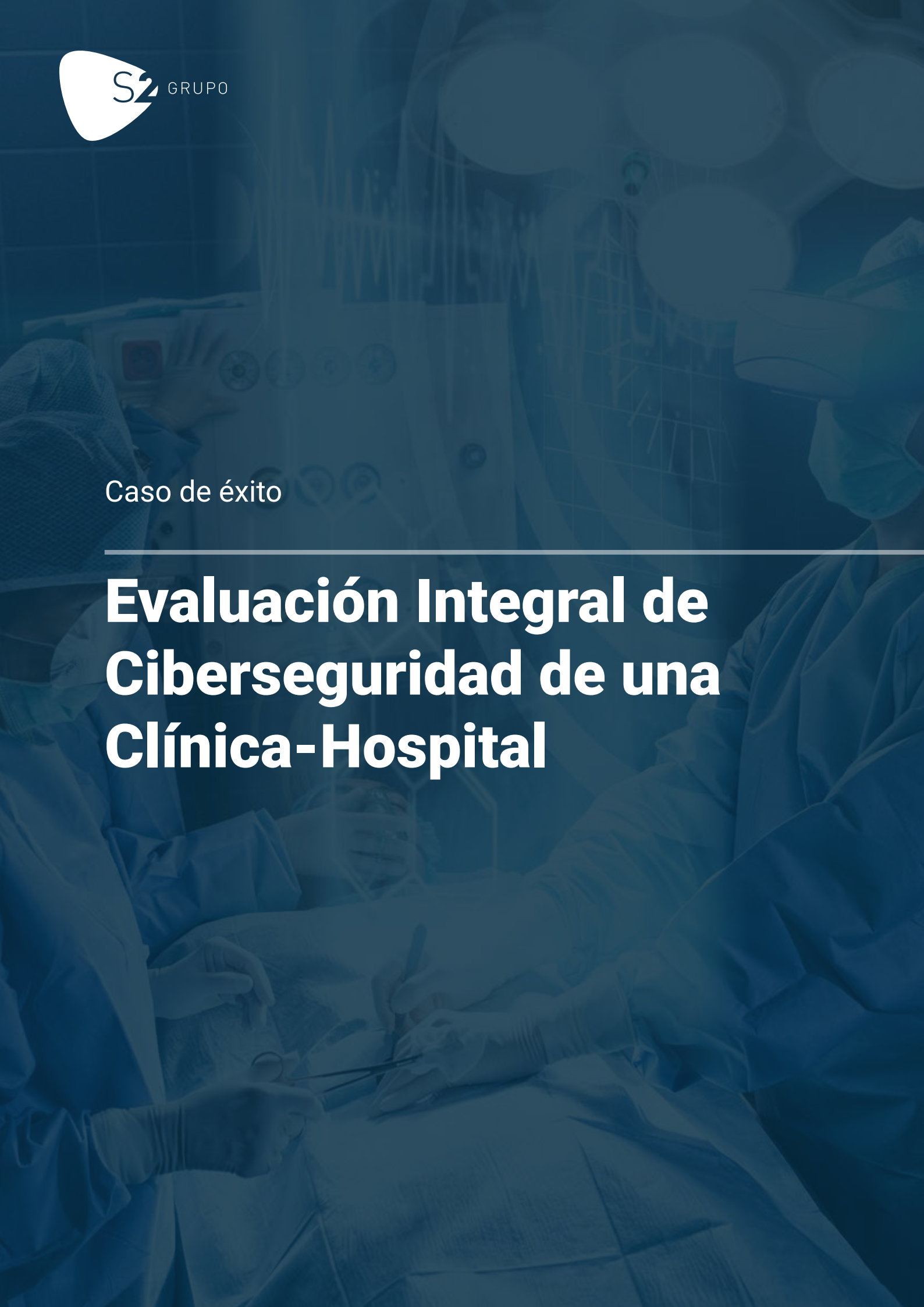

Caso de éxito

Evaluación Integral de Ciberseguridad de una Clínica-Hospital

01

Breve presentación de la empresa:

Nuestro cliente es una compañía internacional de seguros que presta servicios médicos en diferentes países de todo el mundo.

Consciente de los riesgos de ciberseguridad en el sector sanitario la empresa encargó, hace tiempo, a **S2 Grupo** la elaboración de una Guía de Seguridad corporativa. Con un enfoque integral el documento reúne tanto controles de seguridad de la información en las Redes de Comunicaciones (IT) como para los Dispositivos Médicos y los Sistemas de Gestión de los Edificios (OT).

Distribuidos en una serie de Dominios, el documento dispone de hasta 69 puntos de control de las infraestructuras sanitarias.

02

Problemática/reto

Se comprueba que en los últimos años ha habido un **progresivo incremento de incidentes de ciberseguridad en clínicas y hospitales de todo el mundo** con fuga de datos sensibles, daños reputacionales y el bloqueo de la prestación de servicios médicos. Con un evidente daño a la seguridad del paciente y la privacidad de su información personal.

La compañía pretende extender este **marco de ciberseguridad** a toda la organización. Como caso práctico inmediato se decide realizar una evaluación completa de una de sus infraestructuras tomando la Guía de Seguridad corporativa como documento de referencia.

En función de los resultados obtenidos será posible tener un **diagnóstico del estado real de una de las instalaciones** de la organización y que podrá ir extendiéndose a otras infraestructuras sanitarias de la empresa hasta obtener una muestra representativa del estado general.

03

Actuación realizada

Se recopila y analiza la documentación disponible de las redes de comunicaciones, dispositivos médicos e instalaciones de la infraestructura evaluada.

Se realiza una visita al hospital en evaluación con la realización de entrevistas a los responsables de los diferentes departamentos. Además se mantienen reuniones y entrevistas con responsables de proveedores y empresas externas que soportan el funcionamiento de los servicios de la clínica.

El centro cuenta con servicios de urgencias, plantas de hospitalización, cirugía, UCI, imagen diagnóstica, laboratorio clínico y los servicios auxiliares complementarios.

Durante el desarrollo de estas etapas nuestros expertos pueden comprender el funcionamiento de los diferentes departamentos y sus servicios. Identificando los riesgos de ciberseguridad con impacto potencial en la seguridad del paciente, con especial atención a los dispositivos médicos y los sistemas OT de la infraestructura sanitaria (suministro de energía, climatización, seguridad,...).

En la etapa final se realizaron una serie de pruebas técnicas de visibilidad en las diferentes redes de comunicaciones y los dispositivos médicos interconectados.

Pudo comprobarse que las redes de comunicaciones no estaban segmentadas compartiendo la misma red los equipos IT, los dispositivos de radiología e imagen médica y los equipos OT. Aspectos relacionados con la gestión de credenciales, visibilidad entre dispositivos, red wifi y la gestión con proveedores eran claramente mejorables.

Los sistemas encargados de la gestión de la información del paciente compartían la misma infraestructura con los servicios de Radiología, Laboratorio, dispositivos médicos y resto de instalaciones del edificio.

Como resultado de las pruebas realizadas se detectaron muchos puntos que era necesario corregir y mejorar. No se adecuaban a lo especificado en la Guía de Seguridad corporativa. Se redactó un informe que recogía la relación de operaciones realizadas, las deficiencias observadas y una serie de medidas correctoras recomendadas.

Beneficios obtenidos

Con la realización de este proyecto el cliente:

1. Ha podido comprobar el estado real de una de sus infraestructuras poniendo de manifiesto las deficiencias con respecto al marco de ciberseguridad de la organización.

2. Puede corregir los problemas observados en esta instalación adoptando las medidas propuestas y mejorando considerablemente el grado de exposición de esta instalación. Se recogían hasta 54 medidas recomendadas clasificadas tanto como quick wins cómo con prioridades “alta”, “media” y “baja”.

3. Además, desde esta primera evaluación en uno de sus centros, puede extender al resto de instalaciones de la organización las medidas aquí propuestas. Haber constatado la presencia de estas deficiencias le permite entender dónde se encuentran los puntos más críticos de la seguridad de la empresa y de forma fácil e inmediata identificar los problemas habituales. Del mismo modo le ha permitido poner a prueba el documento corporativo de referencia y en su caso mejorarlo para futuras evaluaciones.

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