S2 GRUPO

Anticipando un mundo **ciberseguro**

CASO DE ÉXITO

# **Formación** en **respuesta** ante **incidentes**

01

# Introducción

Se trata de una de las empresas de bienes de consumo más grandes de Perú, aunque dispone de sedes también en el resto de Latinoamérica. La compañía dispone de distintas líneas de negocio y más de 150 marcas propias.

La compañía dispone de un **equipo de ciberseguridad liderado por el CISO**. Sus funciones hasta ahora se han enfocado de forma mayoritaria a la ciberseguridad en el ámbito IT.

Disponen de un sistema documental relativo a ciberseguridad centrado principalmente en el Plan de Respuesta ante Incidentes. Asociado al mismo, cuentan con diversos playbooks IT.

02

# Problemática/reto

La compañía ha realizado anteriormente ejercicios y talleres para formar a todos los trabajadores en el proceso de actuación frente a un posible incidente de ciberseguridad.

Necesita realizar ejercicios a nivel técnico y ejecutivo que **representen un ciberincidente simulado que pudiera darse exactamente igual en la realidad**. Además, toda la información que se utilice para llevar a cabo los ejercicios debe poder darse de la misma forma en un caso real.

Los ejercicios se plantean en un **formato mixto** (un grupo de personas asiste en remoto y otro grupo de personas en presencial) por lo que debe adecuarse la sesión para ambos formatos.

03

# Actuación realizada

Se analizan todos los documentos relativos a la respuesta ante incidentes (plan de respuesta ante incidentes y playbooks) para diseñar unos **talleres previos al simulacro para el equipo de técnicos y ejecutivos**. El objetivo de estos talleres es que todos los trabajadores conozcan el contenido de cada documento y sus funciones y responsabilidades en el caso de materialización de un incidente. Al finalizar estos talleres, todos los trabajadores deben ser capaces de responder de forma adecuada ante un incidente de ciberseguridad.

Para llevar a cabo estos talleres, 3 personas del equipo de seguridad industrial de S2 Grupo se desplazan a las instalaciones del cliente en Perú.

Posteriormente a los talleres, se planifica la ejecución de tres ejercicios de simulación.

Los ejercicios de simulación tienen como **objetivo principal poner a prueba la preparación y capacidad de la compañía** para enfrentar y gestionar incidentes de ciberseguridad, evaluando la efectividad de los procedimientos, políticas y recursos disponibles en la detección, análisis, contención y recuperación de incidentes, así como la toma de decisiones estratégicas.

Se diseña un **ejercicio de simulación basado en un posible caso real**. Para ello, se llevan a cabo reuniones con diversos departamentos dentro del cliente (comunicación, riesgos, operaciones, distribución, etc) con el objetivo de obtener toda la información necesaria para modelar el ejercicio lo más cercano a la realidad posible.

Se convocan **tres ejercicios diferenciados** (dos de ellos dirigidos a técnicos y uno dirigido a ejecutivos). El objetivo es que el incidente se detecte por el equipo de técnicos en la primera sesión, se siga trabajando en él en la segunda, y se reporte al equipo ejecutivo (Comité de Crisis) en la tercera de ellas.

Para ello, se centra el caso en una **infección por ransomware**, incluyendo todas las fases del proceso.

La dinámica de los ejercicios es la misma para todas las sesiones. Se presentan diferentes escenarios en orden cronológico y los asistentes deben ir tomando decisiones en base a inyectores y siguiendo el plan de respuesta ante incidentes de la compañía. Los inyectores son información nueva que va entrando al proceso y que requiere de una actuación por parte del equipo de respuesta ante incidentes.

Para llevar a cabo estos ejercicios, 3 personas del equipo de ciberseguridad industrial de S2 Grupo se desplazan a las instalaciones del cliente en Perú.

Dado que todas las sesiones son impartidas por estas 3 personas, se destina una de ellas para la atención al personal que asiste a la sesión en remoto.

Como resultado de los ejercicios, se realiza un **informe ejecutivo** donde se incluye una descripción general de los mismos, el listado de participantes, las lecciones aprendidas durante los mismos donde se detallan las fortalezas y debilidades encontradas, así como recomendaciones para ejercicios futuros.

04

# Beneficios obtenidos

Con la realización de este proyecto el cliente:

- Verifica de manera didáctica que **todos sus trabajadores son conocedores del plan de respuesta ante incidentes** de la compañía, así como de los playbooks asociados a él.
- Verifica de manera didáctica que **todos los trabajadores son conocedores de sus roles y funciones** dentro del plan de respuesta ante incidentes.
- Verifica de manera didáctica que tanto el **plan de respuesta a incidentes como los playbooks asociados están actualizados**.

S2 GRUPO

MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLA
SAN SEBASTIÁN

SANTIAGO DE CHILE
C.D. MÉXICO
BOGOTÁ
LISBOA
RÓTERDAM

Síguenos en: @s2grupo • s2grupo.es