

■ CASO DE ÉXITO

Servicio de Oficina de concienciación

01

Introducción

Se trata de una de las empresas líderes en el **mercado energético español**, suministradora de electricidad y gas en este y otros mercados energéticos europeos, así como productos de valor añadido del sector energético.





La plantilla cuenta con cerca de 10.000 empleados y da servicio a más de 10 millones de clientes de forma continuada.

Además de la infraestructura para la gestión del correcto funcionamiento de la organización, dispone de una **amplia estructura industrial dedicada a la generación, logística y control de energía constante.**

02

Problemática/reto



La compañía dispone de personal especializado en garantizar unas condiciones de seguridad IT y OT en lo relacionado con la ciberseguridad interna.

Sin embargo, **no tiene un plan de cultura de seguridad eficaz** que ayude a incrementar el nivel global de la seguridad de la compañía y disminuya el riesgo de incidentes relacionados directamente con uno de los componentes clave en esta materia: las personas.

Hay una **necesidad en concienciar, formar y entrenar de manera continuada a las personas** que trabajan en la organización sobre qué situaciones o circunstancias pueden comprometer la seguridad, y además en formarles en modelos de prevención y protección asociados a riesgos específicos.

03

Actuación realizada

Un equipo de expertos de concienciación en ciberseguridad de S2 Grupo, gestiona desde hace más de 10 años la Oficina de Seguridad de la información del cliente en la que se abordan riesgos asociados a las personas en el ámbito IT y OT. Se trata de un servicio continuado cuyo fin es **mejorar las conductas de las personas hacia la ciberseguridad** a través de acciones de:

- **CONCIENCIACIÓN:**

Para involucrar e implicar a las personas en la protección de las tecnologías e información que gestionan. Se muestra a las personas las **amenazas a las que se enfrentan y su posible impacto** haciéndolas entender por qué deben realizar una gestión adecuada de la seguridad.

- **FORMACIÓN:**

A través de la formación se traslada el conocimiento necesario para poner en práctica una **gestión adecuada de la seguridad**. Se les forma en cómo hacerlo.

- **SIMULACIÓN:**

Mediante la ejecución de acciones de entrenamiento se ayuda a las personas a **mantener actualizados sus conocimientos** para hacer una gestión eficaz del riesgo.





Entre las principales tareas realizadas desde la oficina de seguridad destacan las siguientes:

1. **Elaboración de planes de concienciación anuales** teniendo en cuenta los riesgos específicos a los que están expuestos los colectivos de la organización y el análisis del impacto de las acciones realizadas previamente.







2. Dentro de estos planes se incluyen acciones con capacidad para impactar al mayor número de personas mediante contenidos originales y cercanos a situaciones personales que evitan el uso de tecnicismos. Para ello, **se**

combina lo emocional con lo racional, con lo que se consigue que las personas tomen realmente conciencia de los riesgos y de la necesidad de evitarlos.

3. **Gestión de canales** como el site interno, análisis de tráfico e impacto, publicación de contenidos y soporte diario de email ante dudas e incidencias recibidas en el buzón de la oficina.

4. **Generación de informes** que ayuden a la toma de decisiones sobre qué riesgos tratar y a qué colectivos.

Algunos de los **datos relevantes**:

-  42 sesiones de empleados y 8 sesiones infantiles.
-  Valoración media por sesión: 4.8/5.
-  Más de 5.000 impactos de concienciación en sesiones.
-  Número de suscriptores del Site de Seguridad: +1500 suscriptores al site de seguridad.
-  Más de 1100 consultas resueltas.
-  Más de 1000 noticias enlazadas.

04

Beneficios obtenidos

Con la realización de este servicio se ha podido:

- ✓ Disponer de una **oficina de concienciación en seguridad de la información** que de manera continuada dé soporte al equipo de seguridad y ayude a la toma de decisiones sobre los riesgos a tratar en el ámbito IT y OT.
- ✓ Disponer de una **estrategia de comunicación eficaz** que permita optimizar los contenidos elaborados haciéndoselos llegar al empleado de forma atractiva y sencilla y potencie los mensajes y buenas prácticas en seguridad.
- ✓ Disponer de un **canal de comunicación especializado** como referente dentro de la organización sobre cultura de seguridad de la información.
- ✓ **Aumentar el grado de reporte de posibles amenazas** en su CAU de soporte.
- ✓ Conseguir que las personas adopten **prácticas de comportamiento seguro** en seguridad abordando la necesidad de gestionar riesgos en su ámbito más cercano, el ámbito personal y familiar para luego trasladar los mismos riesgos al ámbito corporativo.
- ✓ Conseguir **incrementar el nivel en seguridad** mediante la mejora de la cultura en ciberseguridad.



MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLA
SAN SEBASTIÁN

SANTIAGO DE CHILE
C.D. MÉXICO
BOGOTÁ
LISBOA
RÓTERDAM

Síguenos en:



• @s2grupo

• s2grupo.es