S2 GRUPO
Anticipando un mundo **ciberseguro**

CASO DE ÉXITO

Capacitación en ciberseguridad

colectivos críticos TI

01

Introducción

Empresa multinacional líder en el sector de seguros y servicios financieros con una presencia significativa en todo el mundo. La empresa se ha diversificado en una amplia gama de áreas de seguros, incluyendo seguros de automóviles, seguros de salud, seguros de vida, seguros de hogar,

seguros de empresas, y mucho más. A lo largo de su historia, la empresa ha expandido sus operaciones a nivel mundial y se ha convertido en una de las **principales aseguradoras en América Latina y Europa**, operando en más de 40 países.

La multinacional distribuye sus productos a través de una red de oficinas propias, agentes de seguros, corredores de seguros, bancos, alianzas estratégicas y canales en línea. La empresa utiliza una **variedad de canales** para llegar a sus clientes, lo que le permite adaptarse a las preferencias y necesidades de **diferentes segmentos de mercado.**

La distribución de sus productos y servicios se logra a través de una **infraestructura** de **TI robusta y confiable** que incluye herramientas como servidores, sistemas de información y comunicaciones, bases de datos y aplicaciones, dirigidas y controladas por miles de empleados con **formación estándar en el área de la ciberseguridad**.

02

Problemática/reto

La empresa al desarrollar varios productos y servicios que comportan el uso de **información confidencial** de sus clientes necesita que toda su plantilla, más de 2000 empleados, tenga una **formación básica en ciberseguridad**.

El grupo de empleados expertos, por su nivel de riesgo, están considerados como **colectivo crítico**, por lo que se necesita formación especializada que ayude a profundizar en los conocimientos específicos y **reducir el nivel de riesgo**.

03

Actuación realizada

Un equipo de expertos en ciberseguridad de S2 Grupo junto con los expertos de TI del cliente realiza un análisis del nivel de formación en **ciberseguridad** existente en la empresa para poder identificar las **necesidades formativas** tanto a nivel global como en las **áreas expertas.**

En esta fase de diagnóstico de las necesidades se construye un **modelo basado en competencias de ciberseguridad** (conocimientos, habilidades y actitudes) que favorecen el re-skilling y up-skilling de los empleados IT de la compañía, en concreto:

• Con el re-skiling se consigue el aprendizaje de **nuevas competencias y habilidades de ciberseguridad** para desempeñar con eficacia una **nueva función** dentro de la organización, con el objetivo de **mejorar** las **competencias en ciberseguridad**, clave para afrontar los riesgos, amenazas, retos y oportunidades del empleado IT en un nuevo puesto de trabajo.

• Mediante el up-skilling se facilita y favorece la empleabilidad mediante el **aprendizaje continuo**, realizando programas de capacitación y oportunidades de **desarrollo profesional** con el objetivo de dotar a los profesionales IT de las **habilidades y competencias de ciberseguridad** necesarias en cada momento.

Tras el resultado del análisis se definen las formaciones a realizar a los distintos colectivos IT, la preparación de los contenidos y la coordinación de las formaciones. Esta primera fase del proyecto se concluye con la creación de una primera **formación esencial de ciberseguridad** que engloba a **todos los empleados IT** de la compañía, siendo el punto de partida del plan de formación de la compañía para que todos los empleados tengan un nivel fundamental de conocimiento en ciberseguridad.

La segunda fase se dirige a **formar a las áreas expertas**, para que sean capaces de gestionar los riesgos que competen a cada una de ellas. Se crean **formaciones específicas** para seis áreas concretas del ámbito de la ciberseguridad. El resultado son la impartición de **nueve formaciones en directo**. Todas ellas se han llevado a cabo para grupos de empleados ubicados en todo el mundo. El alcance de este plan de formación comprende un total de 220 webinars en los diferentes idiomas, formando en diferentes materias específicas a más de 6.000 empleados.

04

Beneficios obtenidos

Con la realización de este proyecto el cliente:

- Dispone de un modelo de **competencias en ciberseguridad** que permite involucrar al empleado IT en la gestión del riesgo.
- Establece **itinerarios formativos específicos** para cada colectivo IT dependiendo de sus responsabilidades en materia de ciberseguridad.
- Combate la falta de **talento**, formando y capacitando a los empleados IT para ser más **competitivos**, impulsando la **adaptación** al cambio y la **actualización** del conocimiento de los empleados IT.
- En definitiva, dispone de una **estrategia** que a largo plazo incluye acciones conducentes a la mejora de las competencias del profesional TI.

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