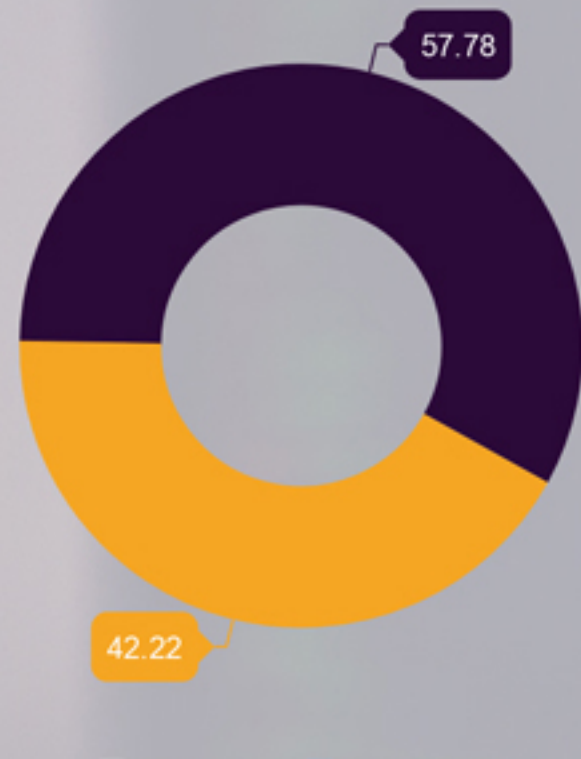


DIRECTIVAS DE SEGURIDAD EN LAS EMPRESAS TURÍSTICAS

Un análisis de las brechas de seguridad en los equipos informáticos de las empresas turísticas que abre el comportamiento no consciente de los empleados.

Preocupación por la seguridad



En líneas generales se observa como la mayoría de los encuestados están sensibilizados con la ciberseguridad (57,78%).

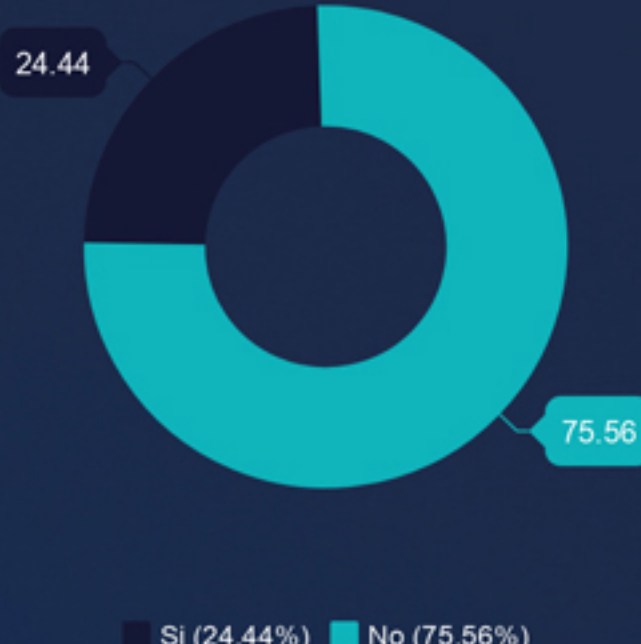
A pesar de ello, un 42 % de los encuestados visitan desde los equipos informáticos de la empresa sus redes sociales en algún momento de su jornada laboral.

Como consecuencia, abren brechas de seguridad en los equipos no siendo conscientes del peligro subyacente.

Consulta de las redes sociales desde los equipos del trabajo



Claves compartidas con otros dispositivos



Se observa como a pesar de la información sobre el peligro de compartir claves de acceso para diferentes dispositivos y aplicaciones, un 24,44% de los empleados en el sector turístico continúan compartiendo estas claves.

Comparte información sobre su empresa



No todas las brechas de seguridad que se abren en una empresa están relacionadas con los equipos informáticos, un 42 % de los encuestados afirma compartir información sobre su organización fuera del entorno laboral.

Se lleva archivos de la empresa a casa



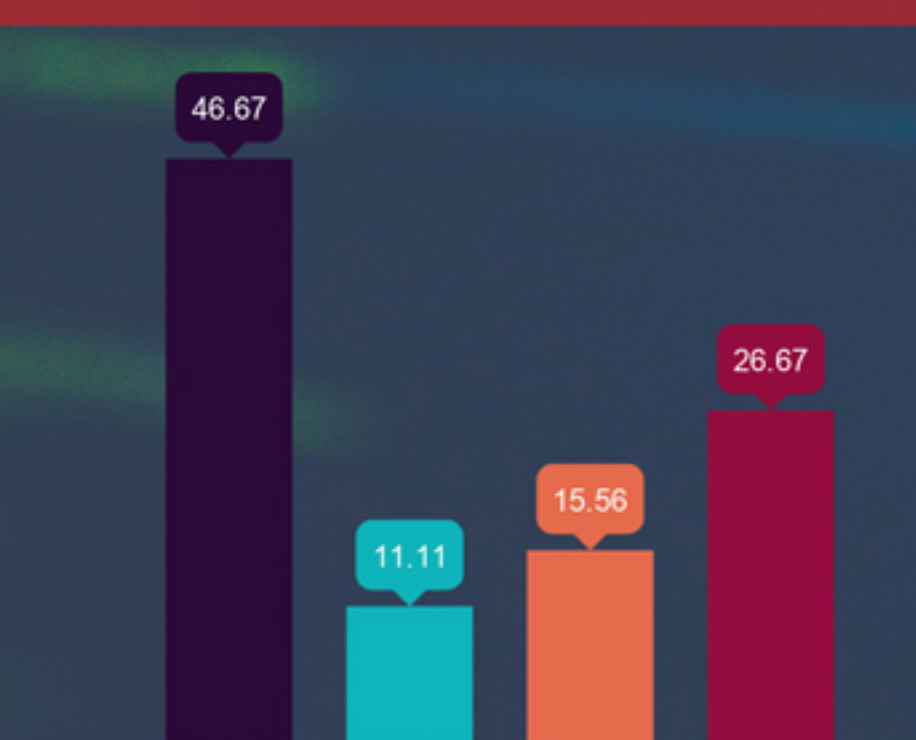
El 29% de los encuestados en alguna ocasión se lleva trabajo a casa. Esto no solo implica una salida de información de la empresa, si no que esta información pueda ser tratada desde equipos que no estén correctamente protegidos.

Consulta de contenido personal



Un 86,67% de los encuestados reconocen consultar contenido en la red de tipo personal en los equipos informáticos de la empresa.

Descarga de archivos



Un 53% de los encuestados admite descargarse archivos no relacionados con su actividad profesional desde los equipos informáticos de la empresa.

La ciberseguridad comienza a ser una de las preocupaciones de los empleados en el sector turístico. Los últimos ataques perpetrados en grandes cadenas hoteleras, han supuesto un incremento de la sensibilidad hacia este tipo de delitos.

A pesar de esta situación la desinformación y el hecho de que el ciberdelincuente siempre vaya por delante a las medidas de seguridad adoptadas, los empleados de una forma no consciente mantienen hábitos que abren brechas de seguridad en los equipos informáticos de la empresa.

POR TANTO, se hace necesario desarrollar planes formativos que se adecuen a la realidad que estamos viviendo. El ciberdelito no es una nueva forma de delinquir. No ha cambiado ni la motivación ni el modus operandi. El delincuente ha ajustado el delito a la nueva era digital.