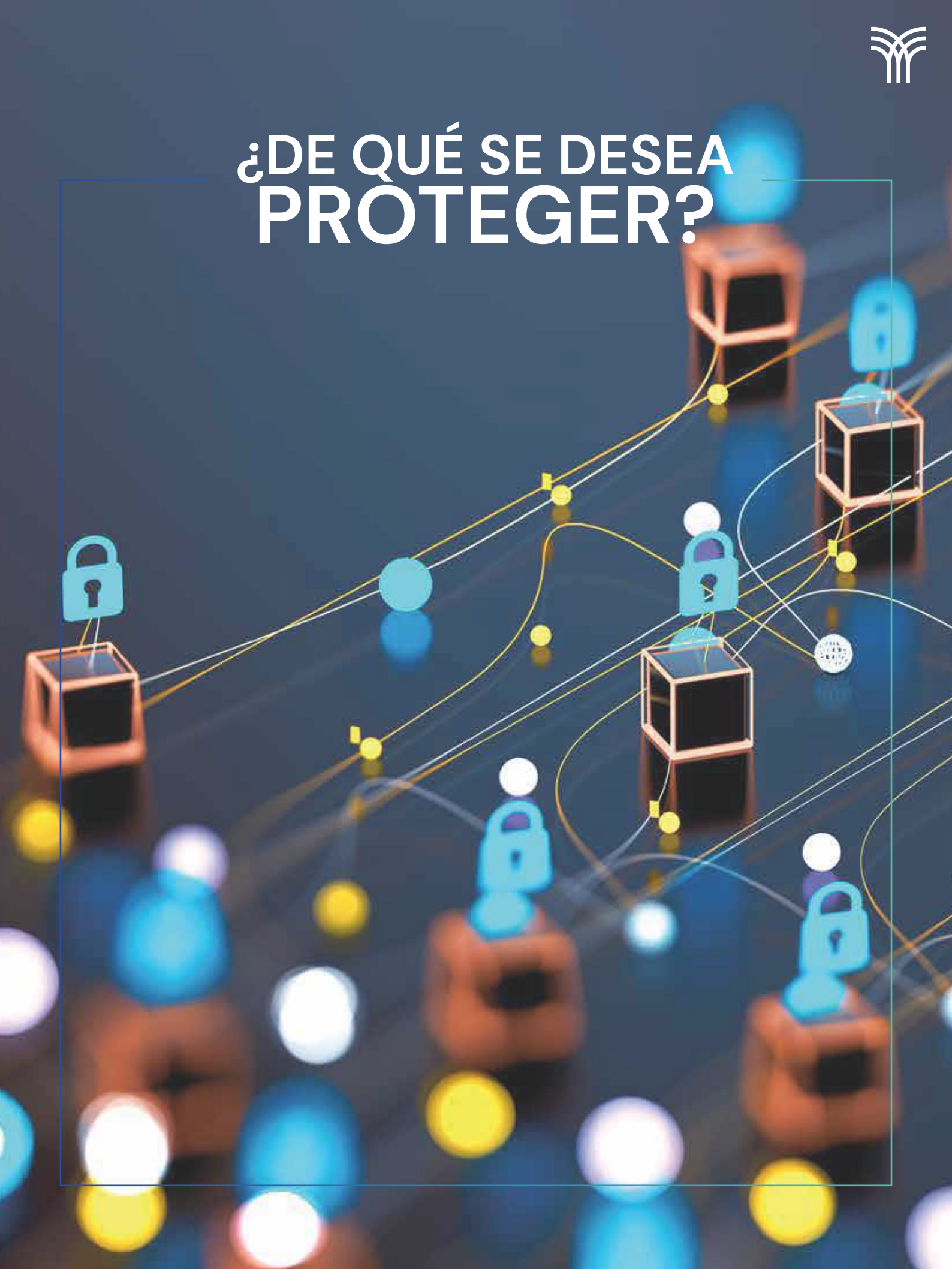
¿DE QUÉ SE DESEA PROTEGER?



¿De qué se desea proteger?

Probablemente, al escuchar la palabra *hacker*, pensemos en el desarrollo de *malware*, robo de bancos, dinero fácil, destrucción de sistemas operativos o robo de información, sin embargo, todas son ideas generalizadas, asumiendo que todos son malos, pero no es así. La idea proviene de muchos factores, como medios sensacionalistas que transforman las noticias e incluso la sociedad que está mal informada.

Un *hacker* es una persona con suficiente conocimiento en algún tema en particular, no necesariamente debe ser informática, puede ser psicología o electricidad. Es una persona que se encarga de tomar todo lo que sabe para poder modificar lo que ya existe y posteriormente darle un uso distinto; le gusta investigar, dominar una técnica, hacerla propia y modificarla. En este caso, hablando de *hackers* informáticos: son aquellas personas que se encargan de perfeccionar, optimizar un servicio o un *script* de programación. Su técnica y mayor motivación es el aprendizaje.

A raíz de la introducción de la informática en los hogares y los avances tecnológicos, ha surgido toda una generación de personajes que difunden el miedo en la red o cualquier sistema de cómputo. Todos ellos son catalogados como "piratas informáticos" o "piratas de la red", también mal conocidos como *"hackers"*, la nueva generación de "rebeldes" de la tecnología que aportan, unos sabiduría y enseñanza, otros destrucción o delitos informáticos.

Hasta la fecha, esta nueva "cibersociedad" ha sido dividida en una decena de grandes áreas fundamentales, en las que reposan con fuerza, la filosofía de cada una de ellas. Todos los grupos aportan, en gran medida, algo bueno en un mundo dominado por la tecnología, pero esto no siempre sucede así. Algunos grupos ilícitos toman estas iniciativas como partida de sus actos rebeldes.

Sombrero blanco
Realizan pruebas de penetración para avisar a los administradores acerca de posibles vulnerabilidades para que las resuelvan a la brevedad posible.

Sombrero azul
Hoy es una variante del sombrero blanco. Se contratan especialistas para realizar pruebas de vulnerabilidad en los sistemas antes de ser lanzados al mercado.

Sombrero rojo
Detectan ataques por parte de hackers de sombrero negro, pero en lugar de notificarlo, inutilizan el ataque de manera silenciosa.

Sombrero negro
Hoy ponen a prueba la seguridad de los sistemas y se aprovechan de las vulnerabilidades encontradas para robar o dañar la información.

Sombrero gris
Es una combinación entre sombrero blanco y negro, tienen los conocimientos para entrar a los sistemas de seguridad y lo pueden utilizar con fines positivos o negativos. En algunas ocasiones ofrecen sus servicios para mejorar la seguridad a cambio de una remuneración económica.