**De la percepción de ilegalidad a la vitalidad**

**en las empresas: hackers en 2023**

CIUDAD DE MÉXICO. XX de marzo de 2023.- La figura del *hacker* durante las últimas dos décadas fue injustamente “satanizada” y generalizada, por culpa de aquellos especialistas en la materia que utilizaban sus conocimientos para vulnerar a otros.

Pero si bien se trata de un especialista al que millones de empresas trataron de evitar durante muchos años, hoy ser *hacker* es uno de los ‘trabajos’ más demandados en todo el mundo.

Un reporte reciente de [LinkedIn](https://www.linkedin.com/pulse/las-10-profesiones-mas-demandadas-para-el-2023-socarras-garcia/?originalSubdomain=es) indica que se trata del quinto perfil con mayor demanda en el inicio de este año, debido al alto nivel de digitalización de los datos de las compañías y de los constantes avances tecnológicos que impactan en su operación diaria. La necesidad de estar protegidos en un plano tan digital, es vital.

Es por eso que los *hackers* dejaron de ser amenazas y potenciales adversarios de las empresas, para convertirse en sus principales aliados. [Randstad](https://www.randstad.es/tendencias360/los-perfiles-mas-demandados-de-2022/) indica en un estudio que los ‘especialistas en ciberseguridad’ pueden ganar hasta $161,000 mensuales.

*“Si las empresas antes destinaban millones de dólares en evitar la presencia de los hackers, hoy deben destinar parte de ese presupuesto en traerlos al interior de sus organizaciones y fomentar la aplicación de técnicas de hacking ético que ayuden a fortalecer los niveles de seguridad que protegen a los datos internos. Ser ‘hackeado’ por los buenos, antes de que los malos lo hagan se ha vuelto esencial”*, destaca Santiago Ronseblatt, CEO y fundador de Strike.

El 2023 será el año en el que las empresas impulsen el trabajo de los profesionales en *hacking* ético altamente calificados, que les ayudarán a encontrar sus vulnerabilidades y solucionarlas. Desde la perspectiva de Strike, empresa líder en ciberseguridad, el cambio hacia el *hacking* ético está liderado por los cambios en los paradigmas de los servicios tradicionales que implican demasiada burocracia, no son transparentes y son poco ágiles y customizables en el proceso de detección.

El *hacking* ético, mediante técnicas como el *pentesting* por mencionar un ejemplo, presenta una propuesta innovadora basada en dejar que un experto en informática se inmiscuya en los sistemas de la empresa como lo haría un ente malicioso, y encuentre las posibles puertas de entrada y debilidades del sistema de una forma que ningún otro especialista lo habría conseguido con métodos convencionales.

Además de tratarse de especialistas con un gran talento y conocimientos, los *hackers* éticos (a los que Strike denomina Strikers) realizan una ejecución ágil y flexible, ya que los encargados de TI pueden modificar aspectos como el alcance, las horas de servicio e incluso el tipo de plan, dependiendo de la forma en la que sus prioridades cambien al ver los primeros resultados.

Los *hackers* éticos, además, mantienen a la compañía siempre notificada de los pasos que realizan durante el proceso mediante reportes transparentes y continuos, lo que hace que el mismo no sólo sea efectivo sino que implique un acompañamiento en tiempo real.

De ese modo, el trabajo del *hacker* ético ha dejado de ser una amenaza para convertirse en parte del ciclo de vida del desarrollo de *software* para las empresas, ayudando a generar capas de seguridad más robustas y un sentido de anticipación ante ataques externos.

El año pasado hubieron amenazas que registraron crecimientos importantes en su incidencia como la vulneración a sistemas en la nube, con un 95%; y la adquisición de credenciales con un 112% según [CrowdStrike,](https://www.crowdstrike.com/global-threat-report/??utm_campaign=globalthreatreport&utm_content=109082_em1prosamsapac-txt1&utm_medium=emc&utm_source=mkto) La misma fuente señala que aparecieron 33 nuevos grupos de cibercriminales en el mundo durante 2022. Esto nos indica que, en conclusión, las empresas deben estar conscientes de que, con o sin su autorización, los *hackers* ingresarán a sus sistemas tarde o temprano y es momento de elegir cómo se les involucrará en sus operaciones.

**Sobre Strike**

Strike es la plataforma de ciberseguridad en Latinoamérica. Su principal misión es ayudar a que las compañías estén protegidas a través de la detección y resolución de vulnerabilidades en sus sistemas. Esto se realiza a través de tests de penetración - o pentests - llevados a cabo por su red global de hackers éticos, conocidos como “Strikers”, una comunidad global que reúne a los mejores expertos de ciberseguridad con reconocimientos y certificaciones internacionales. Su objetivo es impulsar una cultura de ciberseguridad de calidad y accesible, en la que la misma sea parte del ciclo de vida de las empresas y no algo estanco o independiente. Más información en: https://strike.sh/

Síguenos en nuestras redes sociales:

Instagram - @strikesecurity

Twitter - @strike\_secure

LinkedIn - Strike

**Contacto para prensa México**

another

Ahtziri Rangel | PR Expert

+ 52 1 55 1395 6970

ahtziri.rangel@another.co