

# Aplicación de la ciencia de datos en la seguridad informática

## Desafíos y oportunidades para la era digital.

Oscar Ramos, de la Facultad de Informática, Electrónica y Comunicación explica como se usa la ciencia de datos en la seguridad informática actualmente.



Por Oscar Ramos, Estudiante de Ingeniería en Informática de la facultad de Informática, Electrónica y Comunicación.

En los últimos meses, el tema de "seguridad informática" ha adquirido gran relevancia debido al avance tecnológico, ya que numerosos sistemas han sido vulnerados por anomalías presentes en diversos tipos de software, generando un impacto negativo en la seguridad y experiencia del usuario. Afortunadamente, la ciencia de datos brinda herramientas que permiten detectar estas anomalías mediante técnicas y estrategias que agilizan su identificación y eliminación de los sistemas afectados.

La ciencia de datos resulta sumamente útil en este contexto, ya que posee la capacidad de analizar grandes volúmenes de datos, proporcionando una visión más precisa y completa sobre los riesgos de seguridad en el entorno digital. En el campo de la informática, contar con algoritmos basados en ciencia de datos resulta fundamental para fortalecer la seguridad de los sistemas y tomar decisiones que faciliten la protección de la información y la prevención de ataques cibernéticos.

Imaginemos una situación hipotética en la que recibimos un enlace sospechoso, disfrazado de un hipervínculo que aparenta dirigirnos a una reconocida plataforma como Instagram, pero cuyo verdadero propósito es extraer nuestros datos de inicio de sesión mediante una técnica de phishing. En este caso, la ciencia de datos puede analizar y evaluar el enlace para determinar si presenta patrones comunes de phishing, como correos urgentes, solicitudes de actualización de información o mensajes de premios.

A pesar de contar con estas herramientas avanzadas basadas en la ciencia de datos, es importante que los usuarios también aprendan a detectar este tipo de amenazas por su propio criterio. Siempre existe la posibilidad de que algún intento de phishing escape a las herramientas de detección, por lo que combinar el juicio personal con estas herramientas fortalece la seguridad en línea del usuario.

Los ciberataques evolucionan constantemente, por lo tanto, es crucial adoptar medidas adaptativas que puedan anticipar y contrarrestar las nuevas amenazas, garantizando así una seguridad óptima y mejorando la experiencia del usuario.

La ciencia de datos ha brindado un apoyo invaluable a los profesionales en el campo de la seguridad informática, al automatizar tareas y permitirles concentrarse en actividades más complejas y consumidoras de tiempo, como la investigación de amenazas avanzadas.

Es importante destacar que, aunque la ciencia de datos sea un instrumento eficaz contra las anomalías, los usuarios tienen la responsabilidad de educarse y protegerse por sí mismos contra este tipo de amenazas que pueden estar presentes en enlaces, documentos, correos electrónicos y redes sociales. Los usuarios deben informarse sobre las amenazas en línea y ser conscientes de cómo navegar de forma segura por Internet.

La colaboración entre profesionales de seguridad informática también desempeña un papel fundamental en la lucha contra estas amenazas. Al trabajar juntos, con su conocimiento especializado, pueden comprender mejor el panorama de la seguridad y detectar de manera más precisa los patrones de malware, lo que les permite implementar soluciones más efectivas para combatir los virus informáticos mencionados anteriormente.

En la actual era digital, es imperativo que seamos cautelosos frente a las amenazas que pueden surgir en Internet, ya que pueden comprometer nuestros datos e incluso suplantar nuestra identidad. Debemos tomar medidas y establecer límites al navegar por la web, para tener un mayor control sobre nuestros datos y ser menos vulnerables a ataques de phishing mediante enlaces maliciosos enviados a nuestro correo electrónico o número de teléfono.