[notasdeprensa.jpg](http://www.mexicopress.com.mx)Publicado en CDMX el 20/07/2023

# [Autenticación multifactor, el nuevo "must" en ciberseguridad: Hillstone Networks](http://www.notasdeprensa.es)

## Una de las principales vulnerabilidades en ciberseguridad es el uso de contraseñas básicas o débiles, además los usuarios tienden a reutilizarlas para diferentes propósitos, lo cual facilita en gran medida el trabajo de los ciberdelincuentes para acceder a cuentas que se encuentran protegidas por un factor único de autenticación

De acuerdo con Hillstone Networks, los ciberatacantes cuentan con diversas técnicas para robar contraseñas, como spyware, keyloggers y otros tipos de malware, así como ataques de phishing. También existen "diccionarios de contraseñas comunes", con los cuales el atacante solamente debe esperar a que coincidan en un proceso automatizado para tener acceso a la cuenta o sistema, esto se conoce como ataque de fuerza bruta. Si esta estrategia falla, se usan ataques de ingeniería social, donde intentan manipular a la víctima haciéndose pasar por entidades de confianza. Al utilizar solo un factor de autenticación, la posibilidad de ser atacado con éxito dependería de las habilidades del delincuente y la efectividad de las herramientas de seguridad que hayan sido implementadas en los dispositivos o la red. A nivel empresarial, el cumplimiento normativo insta a utilizar autenticación multifactor o MFA para aumentar la seguridad al acceder a datos o sistemas. El objetivo es reducir el riesgo de exposición y robo de datos sensibles, ya que si los atacantes lograran obtener la contraseña aún necesitarían del segundo o tercer factor para concretar el acceso. La autenticación multifactor o MFA trabaja con base en tres factores: and #39;Algo que sabes and #39; (contraseñas, PIN, preguntas de seguridad) and #39;Algo que tienes and #39; (celular, Tablet, token) and #39;Algo que eres and #39; (huella, voz, reconocimiento facial, etc.) Se puede inferir que al aplicar los tres niveles de factores la seguridad será mayor, aunque es indispensable considerar la facilidad de uso y la comodidad del usuario. En este sentido, el balance se ha encontrado al utilizar solamente dos factores (2FA), sin embargo, el factor que brinda mayor seguridad es el relacionado a "Algo que eres", debido a que los biométricos rara vez cambian y son más difíciles de falsificar. "MFA es un gran paso para la protección de datos, aunque no se debe dejar toda la carga de seguridad a una buena práctica. De cierto modo se podría comparar con la seguridad de un edificio, tener que usar múltiples llaves para abrir una puerta puede hacerla más segura, pero si no hay nadie ni nada más para impedir o detectar intentos no autorizados, los malhechores tarde o temprano encontrarán la forma de abrirla. Para proteger a las organizaciones de brechas es necesario defender en profundidad, brindar distintas capas con soluciones específicas que hagan sentido y brinden valor a la organización", explicó Rafael Santana, Technical Marketing Engineer en Hillstone Networks. Hillstone Networks ha desarrollado un amplio portafolio de soluciones de ciberseguridad que sumados a un sistema de MFA logran el objetivo de elevar al máximo los niveles de protección. En suma, la autenticación multifactor se ha posicionado como una práctica que no debe faltar en la planeación de ciberseguridad de cualquier empresa, sin embargo, no debe ser utilizada de forma aislada sino como parte de una estrategia integral de confianza cero.

**Datos de contacto:**

Carlos Soto

Comunicación en Movimiento

5532322068

Nota de prensa publicada en: [https://www.mexicopress.com.mx/autenticacion-multifactor-el-nuevo-must-en](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Telecomunicaciones Programación Ciberseguridad

[notasdeprensa.jpg](http://www.mexicopress.com.mx)

[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)