ABA exhorta priorizar la gestión de ciberseguridad ante riesgos actuales

*Sugiere a las empresas del sector financiero y otros sectores productivos emplear las alternativas que ofrece la IA, mantener sus sistemas actualizados, diseñar una estrategia de prevención y respuesta, entre otras acciones.*

**Santo Domingo, Rep. Dom.-** El uso de la inteligencia artificial y de los resguardos de información, la actualización tecnológica constante y la capacitación del personal constituyen algunos de los elementos primordiales a la hora de prevenir y afrontar las amenazas en materia de ciberseguridad, en una realidad mundial cada vez más cambiante.

Así lo asegura la Asociación de Bancos Múltiples de la República Dominicana (ABA) al plantear algunas recomendaciones con la finalidad de contribuir a las mejores prácticas en la gestión de las tecnologías de la información en el sector financiero y otras áreas productivas, como parte de su plataforma de orientación permanente [Yo Navego Seguro](http://www.yonavegoseguro.com.do/).

La ABA expresó su coincidencia con el planteamiento del Foro Económico Mundial en su reciente informe sobre esta área, donde sostuvo que “en un ciberespacio complejo caracterizado por incertidumbres geopolíticas, una creciente inequidad cibernética y amenazas cibernéticas sofisticadas, los líderes deben adoptar una mentalidad que priorice la seguridad”.

Dicho informe revela que el 66% de las organizaciones espera que la IA tenga el impacto más significativo en la ciberseguridad en el próximo año, pero solo el 37% informa tener procesos implementados para evaluar la seguridad de las herramientas de IA antes de su implementación, recordó la ABA.

Ante esto, la ABA recomienda, en su portal [www.yonavegoseguro.com.do](https://www.yonavegoseguro.com.do/como-potenciar-la-ciberseguridad-de-una-empresa-con-la-inteligencia-artificial/) emplear las alternativas que ofrece la IA para potenciar la seguridad de las empresas, lo que permitiría reducir los tiempos de respuesta a incidentes, detectar ciberamenazas antes y con más precisión, automatizar la respuesta ante determinadas ciberamenazas conocidas, liberar a los profesionales de seguridad para que se centren en tareas más proactivas y mejorar la posición de seguridad.

En un documento de prensa, destacó que el *ransomware* o secuestro de datos es uno de los principales ciberdelitos y toma como referencia la encuesta State of Ransomware 2024 de la empresa [Sophos](https://news.sophos.com/es-es/), donde se revela que el 59% de las organizaciones abarcadas por el estudio fueron atacadas con esta modalidad en el último año.

El documento destaca que, aunque los índices generales de ataques disminuyeron con respecto a 2023, el impacto sobre las víctimas empeoró y, ante esto, Sophos recomienda identificar las vulnerabilidades, prevenir los errores en la configuración de las herramientas de seguridad y procurar soluciones adaptadas a sus necesidades puntuales, sobre todo en el caso de las micro, pequeñas y medianas empresas.

Adicionalmente, la ABA, sugiere realizar [estrategias](https://www.yonavegoseguro.com.do/importancia-de-las-copias-de-seguridad-en-las-empresas/) para el resguardo de información, tomando en cuenta las diferentes opciones existentes, entre las que figuran los servicios de respaldo en la nube, copias de seguridad externas, softwares de copias de seguridad, sistemas de redundancias o combinaciones de las alternativas anteriores.

La Asociación de Bancos indica que es relevante la implementación de actualizaciones regulares en materia tecnológica, diseñar políticas de contraseñas fuertes, así como educar a los colaboradores sobre las mejores prácticas de seguridad y cómo identificar posibles amenazas, a fin de prevenir errores humanos.

**Dirección de Comunicación y Marketing**

23 de enero de 2025