RESETEAR NO BASTA:

La sanitización de datos es clave para proteger la información en la era digital

Antes de desechar dispositivos, los expertos recomiendan que un proveedor certificado aplique un proceso de eliminación irreversible de su contenido.

TRINIDAD VALENZUELA V.

La arqueología de datos es una disciplina especializada que se dedica a recuperar información desde dispositivos antiguos u obsoletos, incluidos formatos fuera de uso o sin soporte. Permite extraer, analizar y reactivar datos, incluso desde discos dañados por incendios o humedad, lo que evidencia cuán vulnerable es la información almacenada en unidades en buen estado.

"Demuestra que la información almacenada sigue siendo recuperable. Esto la expone a caer en manos indebidas y ser usada en extorsiones o ciberataques, evidenciando un riesgo real para la seguridad de los datos personales y sensibles", dice José Medina, subdirector internacional en CompuSoluciones.

Antes de desechar dispositivos con información propia o de terceros, explica, es clave aplicar una política de sanitización de datos. "Esta debe incluir un proceso claro de disposición segura, realizado por un proveedor certificado, que entregue un comprobante de borrado definitivo", afirma el ejecutivo. Además, se debe utilizar tecnología que cumpla con normas internacionales para asegurar el borrado total en cada unidad de almacenamiento.

Rocío Ortiz, subdirectora de Industrias de Futuro del Centro de Innovación UC, explica que estas políticas son fundamentales para cumplir con la ciberseguridad y proteger la confidencialidad, ya que permiten que la eliminación de datos sea segura e irreversible, evitando que información sensible pueda recuperarse mediante técnicas forenses. "Por ello, es crucial implementar medidas de seguridad durante todo el ciclo de vida de los datos, especialmente en su descarte, traspaso y disposición final", dice Ortiz.

Es vital aplicar medidas de seguridad en todo el ciclo de vida de los datos, sobre todo en su descarte, traspaso y disposición final.

La sanitización de datos no solo hace posible cumplir con la normativa y evitar sanciones, sino que también fortalece la seguridad en TI. Sectores como el financiero, salud y educación están sujetos a regulaciones nacionales sobre protección de datos personales. Incorporada en la estrategia de ciberseguridad, esta práctica complementa otras medidas como el control de identidad, DLP, *firewalls* y planes de recuperación ante desastres (DRP), concluye José Medina.