TRIBUNAL DE ÉTICA MÉDICA DEL VALLE DEL CAUCA

INFORME POSIBLE SUPLANTACIÓN DE CORREO ELECTRÓNICO
19 de mayo de 2025

El día 18 de mayo de 2025 se detectó un posible intento de suplantación de identidad por correo electrónico. El mensaje aparentaba provenir de la dirección tribunaleticamedica@temvalle.org, sin embargo, al analizar el encabezado técnico del correo, se evidenció que fue enviado realmente a través del servidor service.ydl30.com, lo cual indica que el dominio legítimo no fue el origen del mensaje. Este comportamiento es un claro indicio de manipulación con fines posiblemente fraudulentos.

El correo fue además marcado como SPAM por los sistemas de seguridad del servidor receptor, lo que refuerza la sospecha de que se trata de un envío no autorizado o malicioso. La firma del mensaje, atribuida al dominio service.ydl30.com, confirma que la comunicación no provino de los servidores oficiales de temvalle.org, sino de un tercero ajeno.
Este tipo de incidentes representa un riesgo significativo para empresas, instituciones y particulares, ya que puede dar paso a intentos de estafa, filtración de datos sensibles, instalación de malware o solicitudes engañosas de recursos financieros. El uso de direcciones de correo aparentemente confiables, pero enviadas desde servidores externos, puede engañar incluso a usuarios con experiencia, especialmente si los mensajes están redactados con tono profesional o institucional.

Es importante que quienes reciban comunicaciones de dominios oficiales como temvalle.org verifiquen cuidadosamente los detalles técnicos del remitente, eviten responder directamente a mensajes sospechosos, y nunca compartan información confidencial sin confirmación previa por canales verificados.

Este informe tiene como objetivo alertar a terceros, empresas y aliados sobre la existencia de este tipo de prácticas, que podrían ser utilizadas para generar engaños con apariencia legítima. La suplantación de identidad digital representa una amenaza real y creciente, por lo que es crucial mantener una postura proactiva frente a cualquier comunicación inusual o que provenga de fuentes no confirmadas. La prevención y la educación en ciberseguridad son fundamentales para mitigar el impacto de estos fraudes.