

VER MÁS...

NUEVA RESOLUCIÓN DE LA DIAN PONE

MAYOR PRESIÓN A LAS EMPRESAS

POR CUMPLIMIENTO DE FACTURACIÓN ELECTRÓNICA

La nueva Resolución 000202 de la DIAN marca un cambio sustancial en el modelo de facturación electrónica en Colombia, elevando significativamente las exigencias para empresas medianas y grandes. La norma introduce requisitos como la recolección limitada de datos del comprador, la obligación de emitir facturas en tiempo real (con excepción técnica justificada) y la centralización de la información en bases de datos de la DIAN. Estas medidas buscan fortalecer la trazabilidad y automatizar la fiscalización, pero muchas empresas aún no están preparadas, lo que las expone a sanciones severas, incluyendo cierres temporales. La resolución también redefine el rol de los proveedores tecnológicos, exigiendo ahora una mayor integración con los sistemas de la DIAN.

Además, el ecosistema tributario colombiano avanza hacia un modelo de control basado en inteligencia de datos, donde la fiscalización se apoya en algoritmos, alertas automáticas y cruces de información en tiempo real. La baja adopción de herramientas como la base de datos tributaria por parte del sector empresarial evidencia un rezago preocupante, mientras que la obligación de contar con certificación en gestión de seguridad de la información antes de octubre impone un nuevo estándar técnico. Todo esto demuestra una clara intensificación del control fiscal, con un enfoque más automatizado, riguroso y exigente para el sector empresarial.

ROBAN CON MENSAJES FALSOS DE FEDEX, DHL Y MÁS EMPRESAS DE ENVÍOS Y ADUANAS

VER MÁS...



El texto alerta sobre una creciente modalidad de fraude digital en América Latina mediante ataques de *phishing* que suplantan la identidad de reconocidas empresas de mensajería como FedEx, DHL, UPS o Correo Argentino. Los ciberdelincuentes utilizan correos electrónicos, mensajes SMS y plataformas como WhatsApp para enviar comunicaciones falsas que simulan problemas con envíos de paquetes. Aprovechan la apariencia visual y el lenguaje corporativo de estas compañías para inducir a los usuarios a entregar datos personales o financieros, bajo tácticas de ingeniería social que apelan al miedo y la urgencia. Casos recientes revelan cómo estas estafas dirigen a sitios web falsos que solicitan información confidencial, afectando a personas desprevenidas.

Frente a esta amenaza, las empresas de mensajería insisten en que nunca solicitan información sensible por medios no oficiales. Se recomienda a los usuarios adoptar prácticas de ciberseguridad como verificar si realmente esperan un paquete, revisar detenidamente el remitente, evitar compartir información confidencial, y desconfiar de mensajes urgentes o mal redactados. También se sugiere examinar los enlaces antes de hacer clic y, ante cualquier sospecha, acudir directamente a los canales oficiales de la empresa. La prevención y el sentido crítico son claves para evitar caer en estas trampas cada vez más sofisticadas.

LA RESPONSABILIDAD EN EL ÁMBITO DEL “COMPLIANCE”

VER MÁS...

El texto desarrolla de forma integral la noción de responsabilidad en el ámbito del *Compliance*, entendida como un sistema transversal que no solo busca cumplir con normas legales y éticas, sino prevenir riesgos, detectar irregularidades y reaccionar ante incumplimientos. Esta responsabilidad no se limita a una dimensión jurídica, sino que se manifiesta en tres niveles: (1) jurídico, que abarca consecuencias penales, civiles y administrativas para personas físicas y jurídicas; (2) organizativo, que exige deberes de diligencia, supervisión y control a los directivos; y (3) ético-social, que remite al compromiso de las empresas con valores como la transparencia, sostenibilidad y legitimidad ante la sociedad. Así, el *Compliance* deja de ser un simple mecanismo formal para convertirse en un factor clave de cultura corporativa y gobernanza responsable.

Además, se analiza la distinción entre responsabilidad objetiva y subjetiva, conceptos fundamentales en la imputación de actos ilícitos dentro de las organizaciones. Mientras la responsabilidad subjetiva requiere probar dolo o culpa, la objetiva se basa en el solo hecho del incumplimiento, trasladando el foco desde el individuo a las fallas sistémicas de la empresa. Este enfoque, adoptado en varias legislaciones, exige a las compañías demostrar la existencia y eficacia de sus programas de Compliance para evitar sanciones. El texto concluye que un sistema de cumplimiento normativo eficaz, vivo y adaptado a los riesgos del entorno es hoy una condición indispensable para la sostenibilidad jurídica, ética y reputacional de cualquier organización.



ULTIMÁTUM PARA EMPRESAS DE ELECTRICIDAD: TIENEN HASTA ESTA FECHA PARA RETIRAR CABLES EN MAL ESTADO

VER MÁS...

El Organismo de Evaluación y Fiscalización Ambiental (OEFA) en Perú, ha establecido como fecha límite el 14 de marzo de 2026 para que las empresas concesionarias del servicio de electricidad retiren el cableado aéreo en desuso o visiblemente dañado en zonas urbanas. Esta medida, respaldada por la Ley N.º 31595, busca mitigar riesgos para la seguridad pública y garantizar el cumplimiento de las normativas ambientales en el sector eléctrico. En caso de incumplimiento, las empresas podrían enfrentar sanciones que van desde 5 hasta 20 Unidades Impositivas Tributarias (UIT). El OEFA ha iniciado procesos de supervisión en todo el país y exhorta a las empresas a actuar dentro del plazo para evitar multas.

Paralelamente, el Ministerio de Transportes y Comunicaciones (MTC) reportó la remoción de más de 200 toneladas de cables en desuso, beneficiando a más de 16,600 calles a nivel nacional, principalmente en Lima y Piura. Estas acciones se desarrollan en colaboración con empresas de telecomunicaciones y gobiernos locales, y se enmarcan en un plan nacional para promover entornos urbanos más seguros, limpios y sostenibles. Además, el MTC viene capacitando a municipalidades para reforzar sus capacidades de supervisión, reiterando su compromiso con la seguridad ciudadana y la mejora del espacio público.