



DOCUMENTO 005 - Política de Protección de Datos

Propósito

AMCA Technologies se compromete a proteger la información de sus clientes, usuarios y terceros relacionados con los servicios de facturación electrónica, conforme a la legislación aplicable en la República Dominicana, los requerimientos técnicos de la Dirección General de Impuestos Internos (DGII) y buenas prácticas internacionales de seguridad de la información.

Esta política define como se recopilan, usan, conservan, protegen y eliminan los datos tratados por AMCA Technologies en la operación de AMCA y sus servicios de Comprobantes Fiscales Electrónicos (e-CF).

Alcance

Esta política aplica a:

Clientes contratantes de AMCA.

Usuarios administradores, contables, operativos y de soporte.

Datos de clientes, proveedores, receptores y emisores contenidos en documentos fiscales.

XML e-CF, acuses de recibo, aprobaciones comerciales, estados DGII, representaciones impresas y bitácoras.

Certificados digitales usados para procesos tributarios cuando el cliente autoriza su custodia o uso en la plataforma.

Procesos de soporte, monitoreo, respaldos, auditoría, seguridad y continuidad operativa.

Quedan fuera del alcance los datos que el cliente procese fuera de la plataforma AMCA o en sistemas terceros que no sean administrados por AMCA Technologies.

Marco Normativo y Referencias

La política toma como referencia:

Ley num. 172-13 sobre protección integral de datos personales en la República Dominicana.

Ley num. 32-23 de Facturación Electrónica.

Ley num. 11-92 que instituye el Código Tributario Dominicano, especialmente los deberes de conservación de soportes tributarios.

Norma General DGII num. 10-2021 sobre certificación de Proveedores de Servicios de Facturación Electrónica.

Roles de Tratamiento

AMCA Technologies puede actuar bajo dos roles según el contexto:

Contexto	Rol de AMCA Technologies	Descripción
Datos comerciales, contractuales, soporte y cuentas propias de AMCA Technologies	Responsable del tratamiento	AMCA Technologies define la finalidad del tratamiento para administrar contratos, soporte, facturación propia, seguridad y relación con clientes.
Datos cargados por clientes en AMCA para su operación y emisión e-CF	Encargado del tratamiento	El cliente define el origen, contenido y finalidad primaria de los datos. AMCA Technologies procesa esos datos dentro de AMCA para prestar el servicio contratado.
Datos fiscales transmitidos o recibidos desde DGII	Encargado técnico / proveedor de servicio	AMCA facilita emisión, recepción, consulta, conservación y trazabilidad de e-CF conforme al modelo operativo DGII.

El cliente mantiene la responsabilidad de validar la licitud, exactitud y autorización de los datos que registra en la plataforma.

Datos Recopilados

AMCA Technologies solo recopila los datos necesarios para operar el servicio, cumplir obligaciones contractuales, fiscales, de seguridad y soporte.

Categoría	Datos tratados	Fuente	Uso principal
Identificación del cliente empresarial	RNC, razón social, nombre comercial, dirección fiscal, teléfono, correo, representantes, empresa y localidad	Cliente / DGII / configuración de AMCA	Alta de cuenta, configuración eCF, emisión fiscal, soporte y auditoría.



AMCA TECHNOLOGIES, S.R.L.

AMCA ERP - Plataforma de Facturación Electrónica e-CF

Calle del Carmen No. 5, Ensanche Naco, Distrito Nacional | +1 (809) 340-8423 | info@amcaerp.com | www.amcaerp.com

	acceso		
Clientes y receptores de e-CF	RNC, cedula, razón social, nombre, dirección, correo, teléfono, condiciones de pago	Cliente	Emisión de facturas, notas, comprobantes y representaciones impresas.
Suplidores y emisores externos	RNC, razón social, datos de contacto, documentos recibidos, acuses y aprobaciones	Cliente / DGII / emisor externo	Recepción, validación y aprobación comercial de e-CF recibidos.
Información fiscal y transaccional	e-NCF, tipo e-CF, fecha, ítems, cantidades, precios, impuestos, descuentos, moneda, tasas, totales, referencias de NC/ND	Operación de AMCA	Generación XML, firma, envío, consulta y conservación fiscal.
XML, PDF y respuestas DGII	XML sin firmar, XML firmado, trackId o número de recepción, respuesta de validación, ARECF, ACECF, PDF representativo, QR	AMCA / DGII	Evidencia fiscal, auditoría, consulta, recuperación y soporte.
Certificados digitales	Certificado autorizado, metadatos de vigencia y credenciales protegidas cuando aplique	Cliente / usuario autorizado	Firma XML e-CF y autenticación contra servicios DGII.
Seguridad y auditoría	Dirección IP, fecha/hora, agente de usuario, acción ejecutada, resultado, errores, cambios de estado	Sistema	Seguridad, monitoreo, investigación de incidentes y trazabilidad.
Soporte	Tickets, mensajes, capturas, archivos adjuntos, diagnósticos técnicos	Cliente / usuario / equipo soporte	Atención de incidentes, mantenimiento y mejora del servicio.
Cookies y datos de sesión	Cookie de sesión, token CSRF, preferencias básicas, identificadores técnicos	Navegador / sistema	Mantener sesión, proteger formularios y mejorar estabilidad.

Finalidad del Tratamiento



AMCA TECHNOLOGIES, S.R.L.

AMCA ERP - Plataforma de Facturación Electrónica e-CF

Calle del Carmen No. 5, Ensanche Naco, Distrito Nacional | +1 (809) 340-8423 | info@amcaerp.com | www.amcaerp.com

servicio	Operación de datos de clientes, proveedores, empresas, respaldos, etc.	Datos de proveedores, estados, etc.
AMCA	contabilidad, impuestos y administración multiempresa.	clientes, documentos y transacciones.
Facturación electrónica e-CF	Generar XML conforme a formato DGII, firmar digitalmente, enviar a DGII y consultar estados.	Datos fiscales, XML, certificado digital, credenciales autorizadas.
Recepción de e-CF	Recibir e-CF de terceros, emitir acuse de recibo, registrar aprobación o rechazo comercial.	XML recibido, datos de emisor/receptor, ARECF, ACECF.
Cumplimiento tributario	Conservar comprobantes, respaldos, evidencias y registros requeridos por DGII.	e-CF, logs, acuses, estados, representaciones impresas.
Seguridad	Prevenir accesos no autorizados, fraude, abuso, errores operativos y pérdida de información.	Logs, IP, roles, permisos, bitácoras y alertas.
Soporte técnico	Diagnosticar errores, asistir al cliente y dar seguimiento a incidentes.	Tickets, trazas, capturas, configuración y logs relevantes.
Administración contractual	Gestionar cuentas, facturación comercial, renovaciones, comunicaciones y SLA.	Datos del cliente, contactos, contrato y plan contratado.
Respaldo y continuidad	Realizar copias de seguridad, recuperación ante fallos y pruebas de restauración.	Bases de datos, archivos XML, adjuntos y configuración crítica.
Mejora del servicio	Analizar errores recurrentes y desempeño del sistema sin usar datos más allá de lo necesario.	Métricas técnicas, errores anonimizados o minimizados.

AMCA Technologies no vende datos personales ni datos fiscales de sus clientes.

Principios de protección

La política se rige por los siguientes principios:

Licitud: el tratamiento se realiza con base contractual, legal, consentimiento o interés legítimo de seguridad.

Finalidad: los datos se usan solo para propósitos definidos y comunicados



AMCA TECHNOLOGIES, S.R.L.

AMCA ERP - Plataforma de Facturación Electrónica e-CF

Calle del Carmen No. 5, Ensanche Naco, Distrito Nacional | +1 (809) 340-8423 | info@amcaerp.com | www.amcaerp.com

Confidencialidad: la información fiscal, personal y comercial se maneja bajo reserva.

Seguridad: se aplican controles técnicos, administrativos y organizativos.

Trazabilidad: las acciones relevantes quedan registradas en bitácoras.

Conservación limitada: los datos se mantienen por el tiempo requerido por ley, contrato u operación.

Responsabilidad demostrable: los controles deben poder evidenciarse ante auditoría o requerimiento.

Diagrama General de Tratamiento de Datos

Etapas	Actor / componente	Tratamiento principal	Control
1	Cliente / usuario autorizado	Ingresa datos operativos, fiscales o de soporte en AMCA.	Autenticación, roles y empresa activa.
2	AMCA frontend/API	Recibe solicitudes y aplica validaciones iniciales.	HTTPS/TLS, sesión segura y validación de entrada.
3	Laravel PHP	Ejecuta reglas de negocio, auditoría y servicios eCF.	Separación lógica, permisos y bitácoras.
4	SQL Server / Azure SQL	Conserva datos transaccionales, estados, usuarios y logs.	Separación por cliente/empresa y respaldos.
5	Azure Blob Storage	Conserva XML, PDF, certificados autorizados y evidencias.	Storage protegido y acceso restringido.
6	Procesos programados e-CF	Procesan envío, consulta DGII y reintentos.	Reintentos controlados, logs y monitoreo.
7	Servicios DGII	Reciben XML firmado y devuelven estados, acuses y aprobaciones.	HTTPS, token y XML firmado.
8	Equipo de soporte autorizado	Atiende tickets e incidentes con acceso limitado.	Mínimo privilegio y trazabilidad del caso.

Cuando existan plazos legales aplicables, estos prevalecen.

Tipo de información	Periodo de conservación	Criterio
e-CF emitidos y recibidos, XML firmado, XML sin firmar, ARECF, ACECF, respuestas DGII, representaciones impresas y bitácoras fiscales	Mínimo 10 años	Conservación tributaria y capacidad de exhibición ante DGII conforme al Código Tributario y normativa e-CF.
Registros contables y soportes vinculados a operaciones fiscales	Mínimo 10 años	Sustento de créditos fiscales, gastos y fiscalizaciones.
Datos de cuenta del cliente y contrato	Durante la relación contractual y el plazo necesario para cumplimiento, defensa o reclamaciones	Gestión comercial, soporte y obligaciones legales.
Usuarios, roles y permisos	Durante vigencia de la cuenta y hasta depuración operativa posterior	Seguridad, auditoría y control de acceso.
Logs de seguridad y auditoría no fiscales	12 a 24 meses como referencia operativa, salvo investigación o requisito legal	Investigación de incidentes, monitoreo y trazabilidad.
Certificados digitales y contraseñas cifradas	Mientras el cliente autorice su uso y el certificado este vigente; eliminación o desactivación al terminar la autorización	Firma XML y autenticación DGII. Se conserva solo evidencia de uso y metadatos necesarios.
Backups operativos	Retención rotativa según política de continuidad, normalmente 30 a 90 días para copias operativas	Recuperación ante incidentes. No se usan como repositorio de consulta ordinaria.
Tickets de soporte y adjuntos	Durante la relación contractual y el periodo necesario para trazabilidad del caso	Soporte, auditoría y mejora del servicio.

Ciclo de Vida de la Información

Etapas	Descripción	Control esperado
1. Recopilación	El usuario o cliente registra datos necesarios para operar el servicio.	Minimización y finalidad definida.
2. Validación	AMCA valida formato, permisos, empresa y reglas fiscales.	Validaciones de entrada, roles y bitácora.
3. Uso operativo	Los datos se usan para facturación, soporte, consulta, reportes y operación e-CF.	Acceso por permisos y trazabilidad.
4. Firma y envío DGII	XML e-CF, ARECF o ACECF se firman y transmiten cuando aplica.	Certificado autorizado, HTTPS y registro de respuesta.
5. Almacenamiento seguro	XML, PDF, estados y respuestas se conservan en SQL Server/Blob.	Separación por cliente/empresa, cifrado cuando aplique y acceso restringido.
6. Respaldo	Se protegen datos críticos mediante backups y retención.	política de respaldo y prueba de restauración.
7. Conservación legal	Los documentos fiscales se retienen por el plazo exigido.	Retención tributaria y capacidad de exhibición.
8. Eliminación o anonimización	Cuando procede, se elimina o anonimiza información no sujeta a retención.	Validación legal, evidencia de acción y cierre.

Cada etapa debe mantener controles de acceso, bitácora, cifrado cuando aplique y separación por cliente o empresa.

Derechos de los Titulares

Los titulares de datos personales pueden ejercer, según corresponda y conforme a la ley:

Acceso: conocer si AMCA Technologies trata sus datos y obtener información sobre dicho tratamiento.

Rectificación: solicitar corrección de datos inexactos o incompletos.

Portabilidad o entrega de información: obtener datos exportables cuando sea técnica y jurídicamente aplicable.

Habeas data: ejercer las acciones previstas por la normativa dominicana.

Las solicitudes se gestionan por el canal de privacidad indicado en esta política. AMCA Technologies puede requerir validación de identidad y, cuando el dato pertenezca a un cliente empresarial, coordinar la respuesta con dicho cliente.

Flujo de Atención de Derechos

Paso	Responsable	Acción	Evidencia
1	Titular	Presenta solicitud de acceso, rectificación, supresión u otro derecho aplicable.	Correo o ticket recibido.
2	Privacidad AMCA Technologies	Valida identidad, alcance y relación con cliente/empresa.	Registro de validación.
3	Cliente responsable, si aplica	Confirma autorización o criterio cuando el dato pertenece a su operación.	Respuesta documentada.
4	AMCA ERP / equipo autorizado	Localiza datos relevantes y restricciones legales.	Resultado de búsqueda y soportes.
5	Privacidad AMCA Technologies	Registra decisión, acción aplicada y base de conservación si existe.	Bitácora o expediente de privacidad.
6	Privacidad AMCA Technologies	Responde al titular por el canal definido.	Comunicación de cierre.

Medidas de Seguridad

AMCA Technologies aplica controles de seguridad proporcionales al riesgo de los datos tratados.

Controles Técnicos

Cifrado en tránsito mediante HTTPS/TLS para acceso a AMCA y comunicación con servicios externos.



AMCA TECHNOLOGIES, S.R.L.

AMCA ERP - Plataforma de Facturacion Electronica e-CF

Calle del Carmen No. 5, Ensanche Naco, Distrito Nacional | +1 (809) 340-8423 | info@amcaerp.com | www.amcaerp.com

Limitación de tasa en servicios públicos utilizados para integración e-CF.

Cifrado de contraseñas de certificados digitales y secretos sensibles mediante mecanismos seguros del framework.

Almacenamiento de XML y archivos fiscales en repositorios controlados.

Bitácoras de auditoria para estados e-CF, envíos, consultas y cambios relevantes.

Backups periódicos de bases de datos y archivos críticos.

Monitoreo de errores, disponibilidad y vencimiento de certificados digitales.

Controles Administrativos

Acceso restringido al personal autorizado.

Principio de mínimo privilegio.

Revisión de accesos cuando cambian roles o termina una relación laboral o contractual.

Procedimientos de soporte que evitan exponer datos innecesarios.

Acuerdos de confidencialidad para personal con acceso a información sensible.

Gestión documentada de incidentes y requerimientos de información.

Controles sobre Certificados Digitales

El certificado digital pertenece al contribuyente o representante autorizado.

El uso del certificado en AMCA ERP requiere autorización expresa del cliente.

El certificado y su credencial de uso no deben almacenarse en texto plano.

La plataforma mantiene alertas de vencimiento y trazabilidad de uso.

Al finalizar el contrato o revocar la autorización, se deshabilita el uso del certificado y se elimina o retiene solo lo estrictamente necesario para evidencia legal.

Diagrama de Seguridad por Capas

Capa	Control	Propósito
Usuario autorizado	Credenciales, sesión y permisos	Evitar acceso no autorizado.
Canal HTTPS/TLS	Cifrado en tránsito	Proteger datos entre navegador, API y servicios externos.



AMCA TECHNOLOGIES, S.R.L.

AMCA ERP - Plataforma de Facturación Electrónica e-CF

Calle del Carmen No. 5, Ensanche Naco, Distrito Nacional | +1 (809) 340-8423 | info@amcaerp.com | www.amcaerp.com

Roles y empresa activa	Autorización funcional	Limitar acciones por rol, cliente y empresa.
Laravel API	Validaciones y reglas de negocio	Procesar solicitudes con controles centralizados.
Aislamiento lógico	Separación lógica de datos	Evitar mezcla de información entre clientes/empresas.
SQL Server / Azure Blob	Persistencia y archivos protegidos	Conservar datos, XML, PDF, certificados y evidencias.
Bitácoras y logs	Auditoría de eventos	Rastrear cambios, envíos, consultas y errores.
Colas e-CF / DGII	Procesamiento controlado por HTTPS	Firmar, enviar, recibir y consultar documentos fiscales.
Monitoreo y alertas	Observabilidad operativa	Detectar fallos, rechazos e incidentes.

Uso de Cookies

AMCA ERP utiliza cookies y tecnologías equivalentes necesarias para el funcionamiento seguro del sistema.

Tipo	Finalidad	Obligatoria
Cookie de sesión	Mantener la sesión autenticada del usuario.	Si
Token CSRF	Proteger formularios y solicitudes contra ataques de falsificación.	Si
Preferencias técnicas	Recordar opciones de interfaz o configuración no sensible.	No siempre
Análítica técnica interna	Medir estabilidad, errores y rendimiento, cuando este habilitado.	Opcional

No se utilizan cookies para vender datos personales. Si se incorporan herramientas de analítica, publicidad o terceros, AMCA Technologies documentará su finalidad, proveedor, duración y mecanismo de exclusión cuando aplique.



AMCA TECHNOLOGIES, S.R.L.

AMCA ERP - Plataforma de Facturación Electrónica e-CF

Calle del Carmen No. 5, Ensanche Naco, Distrito Nacional | +1 (809) 340-8423 | info@amcaerp.com | www.amcaerp.com

servicio, cumplir la ley o atender requerimientos autorizados.

Tercero / categoría	Datos involucrados	Finalidad
DGII	XML e-CF, datos fiscales, acuses, aprobaciones, estados	Validación, recepción y consulta de comprobantes fiscales electrónicos.
Microsoft Azure	Bases de datos, archivos, backups, logs técnicos	Hosting, almacenamiento, respaldo y monitoreo.
GitHub	Código fuente, control de cambios, integración y despliegue	Gestión de desarrollo. No debe almacenar certificados ni datos fiscales productivos.
Proveedores de correo o soporte	Datos de contacto, notificaciones y tickets	Soporte y alertas operativas.

Los terceros deben estar sujetos a controles de acceso, confidencialidad y seguridad razonables para el tipo de información tratada.

Respuesta a Incidentes

AMCA Technologies mantiene un proceso de respuesta ante incidentes de seguridad o privacidad. Para esta política, un incidente es cualquier evento que pueda afectar la confidencialidad, integridad, disponibilidad o uso autorizado de datos personales, datos fiscales, XML e-CF, certificados digitales, credenciales, respaldos, logs o servicios críticos de AMCA.

El sistema de tickets se utiliza como registro operativo y evidencia de seguimiento. También pueden generarse registros complementarios en bitácoras del sistema, monitoreo, correo, actas internas o reportes técnicos cuando el incidente lo requiera.

Etapas	Acción requerida	Evidencia esperada
1. Detección y registro	Registrar el evento en el sistema de tickets o bitácora autorizada. Incluir fecha, hora, usuario reportante, cliente/empresa, módulo afectado y descripción inicial.	Ticket, correo de reporte, alerta de monitoreo o log inicial.

	información. Asignar severidad.	
3. Contención	Aplicar acciones inmediatas para limitar el impacto: bloqueo de cuenta, revocación de token, rotación de credenciales, aislamiento de servicio, suspensión temporal de proceso o restricción de acceso.	Acciones aplicadas, hora de ejecución y responsable técnico.
4. Análisis de impacto	Identificar sistemas afectados, datos involucrados, clientes impactados, documentos e-CF relacionados, periodo afectado y causa probable.	Informe técnico, lista de documentos/registros afectados y logs revisados.
5. Corrección y recuperación	Ejecutar la solución: parche, cambio de configuración, restauración de respaldo, reproceso controlado, reenvió e-CF, ajuste de permisos o reemplazo de certificado.	Evidencia de corrección, prueba posterior y aprobación técnica.
6. Comunicación	Informar a responsables internos, cliente afectado, DGII u otra autoridad cuando aplique por ley, contrato o requerimiento operativo.	Correo, acta, comunicación formal o acuse de notificación.
7. Cierre	Documentar causa raíz, medidas correctivas, medidas preventivas y aprobación de cierre.	Ticket cerrado, evidencias adjuntas y lecciones aprendidas.
Severidad	Criterio	Tiempo objetivo de primera respuesta
Critica	Exposición de datos sensibles, compromiso de certificado digital, acceso no autorizado confirmado, caída total del servicio e-CF o imposibilidad masiva de emitir/recibir comprobantes.	Hasta 1 hora laboral o atención inmediata si existe monitoreo activo.
Alta	Error que afecta un cliente, empresa o proceso fiscal relevante, rechazo masivo DGII, indisponibilidad parcial o sospecha razonable de acceso indebido.	Hasta 4 horas laborales.
Media	Incidente controlado, impacto limitado, falla intermitente o desviación sin evidencia de fuga de información.	Hasta 1 día laborable.



AMCA TECHNOLOGIES, S.R.L.

AMCA ERP - Plataforma de Facturación Electrónica e-CF

Calle del Carmen No. 5, Ensanche Naco, Distrito Nacional | +1 (809) 340-8423 | info@amcaerp.com | www.amcaerp.com

Todo incidente debe conservar, como mínimo, fecha de detección, fecha de cierre, responsable, alcance, sistemas afectados, datos comprometidos si aplica, medidas de contención, acciones correctivas, comunicación realizada y evidencias de cierre. Las medidas preventivas derivadas del incidente se registran como tareas de mejora y se relacionan con el ticket original.

Privacidad desde el Diseño

Los cambios a AMCA ERP deben considerar privacidad y seguridad desde el diseño:

Evaluar si el cambio requiere nuevos datos personales o fiscales.

Evitar duplicar datos sensibles cuando existan identificadores suficientes.

Usar maceramiento o minimización en logs.

Validar que los servicios nuevos respeten cliente, empresa, roles y permisos.

Evitar datos productivos en ambientes de desarrollo.

Documentar nuevos terceros, cookies o transferencias.

Probar que exportaciones y reportes respeten permisos.

Contacto para Privacidad

Las solicitudes relacionadas con privacidad, derechos de titulares o reporte de incidentes deben dirigirse a:

Canal	Detalle
Correo	info@amcaerp.com
Responsable	Dirección de Seguridad y Cumplimiento - AMCA Technologies
Asunto sugerido	Solicitud de Privacidad / Datos Personales
Datos mínimos	Nombre, identificación, empresa relacionada, solicitud concreta y medio de contacto

Revisión y Aprobación

Esta política debe revisarse al menos una vez por año o cuando ocurran cambios materiales en:

Normativa DGII o legislación de datos personales.



AMCA TECHNOLOGIES, S.R.L.

AMCA ERP - Plataforma de Facturacion Electronica e-CF

Calle del Carmen No. 5, Ensanche Naco, Distrito Nacional | +1 (809) 340-8423 | info@amcaerp.com | www.amcaerp.com

Alcance de servicios e-CF.

Rol	Nombre	Firma	Fecha
Direccion General			

Fuentes Oficiales Verificadas

DGII - Facturacion Electronica: <https://dgii.gov.do/cicloContribuyente/facturacion/comprobantesFiscalesElectronicosE-CF/Paginas/default.aspx>

DGII - Documentacion sobre e-CF: <https://dgii.gov.do/cicloContribuyente/facturacion/comprobantesFiscalesElectronicosE-CF/Paginas/documentacionSobreE-CF.aspx>

Ley num. 172-13: <https://dgii.gov.do/transparencia/marcoLegal/Documents/Leyes/172-13.pdf>

Ley num. 32-23 de Facturacion Electronica: <https://dgii.gov.do/transparencia/baseLegal/Documents/Leyes/Ley%2032-23.pdf>

Norma General num. 10-2021: <https://dgii.gov.do/legislacion/normasGenerales/Documents/NG%20sobre%20Comprobantes%20Fiscales/Norma10-21.pdf>

Codigo Tributario Ley num. 11-92: <https://dgii.gov.do/legislacion/leyesTributarias/Documents/Codigo%20Tributario%20y%20Leyes%20que%20lo%20modifican%20y%20complementan/11-92.pdf>