01 Política de Seguridad de la Información

DOCUMENTO OFICIAL · KARMA TECH CONSULTING, S.R.L. · Aprobado por la Dirección · Entrega a la DGII

Código	Versión	Emisión	Revisión
KTC-EFC-POL-SI-001	**1.0**	**12/10/2026**	**Anual**

Documento formal que define los controles de seguridad de la información del servicio e-Fiscal Cloud de KARMA TECH CONSULTING, S.R.L., presentado ante la DGII como parte de la solicitud para ser Proveedor de Servicios de Facturación Electrónica.

1 Declaración de compromiso de la Dirección

La Dirección de **KARMA TECH CONSULTING, S.R.L.** declara su compromiso con la protección de la información que le confían los contribuyentes y la Administración Tributaria, y asume la responsabilidad de proveer los recursos, roles y controles necesarios para la operación segura, continua y trazable del servicio e-Fiscal Cloud, conforme a la legislación dominicana y a las buenas prácticas internacionales (ISO/IEC 27001, ISO/IEC 20000-1, ITIL 4 y COBIT 2019).

1.1 Objetivo y alcance

Establecer los controles que protegen la **confidencialidad, integridad y disponibilidad** de la información procesada por e-Fiscal Cloud: comprobantes fiscales electrónicos (e-CF), acuses de recibo y aprobación comercial, certificados digitales de los contribuyentes, datos de compradores e información tributaria intercambiada con la DGII.

Alcance: portal web de autogestión, API de integración (ERP, POS, comercio electrónico y sistemas empresariales), servicios de firma, envío y consulta de estado, servicio de recepción de e-CF, procesos de notificación, base de datos, infraestructura en la nube y el personal y terceros que intervienen en su operación.

2 Principios y responsabilidades

Rol	Responsabilidad
Dirección	Aprueba esta política, asigna recursos y revisa su eficacia al menos una vez al año.
Responsable de Seguridad y Operación	Implementa los controles, gestiona incidentes, custodia credenciales críticas y mantiene la relación técnica con la DGII.
Equipo de desarrollo	Aplica desarrollo seguro, control de cambios y protección de secretos.
Usuarios y terceros	Cumplen esta política y los acuerdos de confidencialidad; reportan eventos de seguridad.

3 Clasificación de la información

Categoría	Ejemplos	Tratamiento

Crítica / Secreta	Certificados digitales (.p12), contraseñas de certificados, llaves privadas, claves de API, tokens de autenticación ante la DGII	Cifrado en reposo; acceso mínimo y nominal; nunca en bitácoras ni en código fuente
Confidencial	e-CF y su XML, datos del comprador (RNC/cédula, nombre, correo, teléfono), reportes fiscales	Cifrado en tránsito y en reposo; acceso por rol y por empresa
Interna	Configuración, bitácoras, métricas, documentación técnica	Acceso autenticado del personal autorizado
Pública	Documentación de producto, sitio institucional, políticas publicadas	Libre

4 Control de acceso

- **Autenticación nominal** para todo usuario del portal; no se permiten cuentas compartidas. Segundo factor obligatorio para cuentas administrativas.
- **Modelo de roles jerárquico** (administrador de plataforma, administrador de empresa, supervisor, usuario operativo) bajo el **principio de menor privilegio**: cada usuario accede solo a las empresas y sucursales asignadas.
- **Aislamiento multiempresa:** los datos de cada contribuyente se segregan lógicamente y toda consulta se filtra por empresa.
- **Credenciales de integración** (claves de API) emitidas por empresa, revocables y almacenadas con *hash*.
- **Acceso a la infraestructura** restringido por llaves criptográficas y redes autorizadas; sin acceso por contraseña. Altas, bajas y revisiones trimestrales de accesos documentadas.
- **Separación de ambientes:** pre-certificación/certificación y producción aislados, con secuencias e-NCF y datos de prueba separados de los reales.

5 Criptografía y protección de datos

- **En tránsito:** todo el tráfico se cursa sobre HTTPS con TLS 1.2 o superior; no se exponen servicios por HTTP plano.
- **En reposo:** base de datos y respaldos cifrados; las contraseñas de los certificados .p12 se almacenan cifradas y las llaves de firma se cargan solo en memoria durante la firma.
- **Firma digital:** los e-CF, acuses (ARECF/ACECF) y la Declaración Jurada se firman con el certificado del contribuyente mediante firma XML *enveloped* (RSA-SHA256), conforme a los formatos técnicos de la DGII.
- **Gestión de secretos:** claves y tokens se gestionan como variables protegidas fuera del código fuente y nunca se versionan.
- **Ciclo de vida de certificados:** control de vencimientos con alertas anticipadas y procedimiento de rotación controlada.

6 Comunicaciones con la DGII y registro de eventos

- Uso exclusivo del flujo oficial de autenticación: **semilla → firma → validación del certificado → token**; los tokens se almacenan cifrados y se renuevan antes de su expiración.
- Validación del emisor y receptor por **RNC** en los documentos recibidos; los acuses se firman con el certificado de la empresa receptora.
- Cabeceras de seguridad HTTP, validación estricta de entradas y **límite de tasa** en los servicios expuestos.

Bitácora de eventos (trazabilidad)

Registro	Contenido mínimo
Transacciones e-CF	e-NCF, RNC emisor/receptor, fecha y hora, TrackId, estado DGII y respuesta recibida
Accesos y administración	Usuario, acción, empresa afectada, IP, fecha y hora (inicios de sesión, cambios de rol, carga de certificados)
Disponibilidad DGII	Estado de los servicios de la DGII y reintentos, como evidencia verificable de atrasos no atribuibles al emisor
Notificaciones	Canal, destinatario enmascarado, estado de entrega y marcas de tiempo
Cambios	Versión desplegada, responsable, fecha y referencia del cambio

Las bitácoras se protegen contra modificación, sincronizan su hora con una fuente confiable, **nunca registran secretos** y se conservan al menos durante el plazo que exige la normativa tributaria.

7 Desarrollo seguro y gestión de cambios

- Código fuente en repositorio privado con control de versiones; todo cambio es trazable y revisado antes de pasar a producción.
- Pruebas funcionales en ambiente de certificación previo a cada despliegue; dependencias con versiones fijadas y revisadas por vulnerabilidades.
- Despliegues reproducibles con capacidad de **reversión** a la versión anterior.
- Consultas parametrizadas y validación de entradas para prevenir inyección y otras vulnerabilidades comunes.

8 Gestión de incidentes de seguridad

Fase	Acción
Detección	Monitoreo de servicios, alertas y reportes de usuarios por los canales oficiales.
Contención	Aislamiento del componente afectado, revocación de credenciales comprometidas.
Erradicación y recuperación	Corrección, restauración desde respaldo validado y verificación de integridad de e-CF.
Comunicación	Notificación a contribuyentes afectados y, cuando corresponda, a la DGII y a los titulares de datos.
Lecciones aprendidas	Análisis de causa raíz y acciones correctivas registradas.

Canales para reportar eventos de seguridad: **soporte@efiscalcloud.com** · **soporte@karmatechconsulting.com** · **849-379-4444**.

9 Terceros y proveedores

Los proveedores de infraestructura en la nube y servicios de comunicación actúan bajo acuerdos de confidencialidad y seguridad; se evalúan antes de su contratación y se revisan periódicamente.

10 Cumplimiento normativo

- Ley 32-23 de Facturación Electrónica; Norma General 01-2020; Norma General 10-21; Reglamento 587-24.
- Ley 172-13 sobre Protección de Datos de Carácter Personal (ver Documento 03).
- Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología.

11 Revisión

Esta política se revisa al menos **anualmente** o ante cambios significativos de la plataforma, de la normativa o tras un incidente relevante.

Etapa	Responsable	Fecha
Elaborado	Área de Tecnología y Seguridad de la Información — e-Fiscal Cloud	12/10/2026
Revisado	Responsable de Seguridad y Operación	12/10/2026
Aprobado	Stensy Pérez Olivares — Representante autorizado	12/10/2026

Stensy Pérez Olivares
Representante autorizado
KARMA TECH CONSULTING, S.R.L. · RNC 133-04060-3

KARMA TECH CONSULTING S.R.L. RNC 133-04060-3 Santo Domingo, Rep. Dom.