POLÍTICA ANTI-FRAUDE
Para cuentas de Usuario Final

ÍNDICE

1. INTRODUCCIÓN

A los efectos de la presente Política Anti-Fraude, el Usuario Final es la persona, física o jurídica, que establece una relación contractual con Nosotros, aceptando los Términos de Uso y proveyendo contenido que será puesto a disposición de las Plataformas de Streaming Digital (o DSP). “Nosotros” somos los proveedores del servicio, DINASTIA MARKET INC.

El propósito de esta Política es determinar las normas de buen hacer que aplicarán a los Usuarios Finales de nuestros servicios. En ella, se definirán las acciones a emprender como consecuencia de un uso fraudulento de nuestra plataforma.

1.1 Finalidad:

La finalidad de esta Política es establecer lo siguiente:

- Una definición clara de lo que entendemos por “fraude”.
- Una declaración definitiva para rechazar la actividad fraudulenta en todas sus formas.
- Un resumen de las responsabilidades del Usuario Final para evitar actividades fraudulentas.
- Una guía para todas las partes involucradas referente a las medidas que deben tomarse cuando Nosotros, los DSP o un tercero tengamos la sospecha de que se está produciendo una actividad fraudulenta.
- Una guía clara acerca de las responsabilidades para realizar investigaciones sobre actividades fraudulentas.
- Una mayor protección para los titulares de derechos en aquellas circunstancias en las que pudieran ser víctimas de actividades fraudulentas.

Este documento pretende servir de orientación y se debe leer junto con:

- La Política de Privacidad
- Los Términos de Uso

1.2 Objetivo:

El objetivo principal de esta política es prevenir, detectar y responder eficazmente a cualquier forma de fraude que pueda afectar a DINASTIA MARKET INC & DINASTIA MARKET LLC como Distribuidor de música digital.

2. DEFINICIONES

Usuario Final: La persona o entidad legal que ha establecido una relación contractual con DINASTIA MARKET INC para el uso de la plataforma, tras aceptar los Términos de Uso, con el objeto de proveer contenido a las DSP a través de la misma.

Cuenta de Usuario: Cualquier cuenta perteneciente y/o creada por un Usuario Final.

DSP: Son las siglas de 'Digital Streaming Platforms', o Plataformas de Streaming Digital, tales como Spotify, Apple Music o Tidal, así como cualesquiera otros conectados a Nosotros mediante vinculación contractual.

MDFS: Son las siglas de 'Monetization through Digital Fingerprinting Systems', o sistemas de monetización a través de sistemas de huella digital, que son utilizados por YouTube Content ID o Facebook Rights Manager, entre otros.

Fraude: Cualquier actividad contraria a la Ley, las políticas de los DSP o nuestras propias Políticas. Concretamente, y de forma no exhaustiva, consideraremos como Fraude las siguientes actividades:

- La explotación no autorizada de material protegido por Copyright.
- La infracción de cualquier ley reguladora de la Propiedad Intelectual de los titulares de derechos.
- El uso y apropiación de nombres y/o nombres de obras de determinados artistas y bandas, incluidas imágenes de portadas, o nombres de sellos discográficos, siempre que dicho uso pueda crear confusión o falsas expectativas relacionadas con el contenido que los DSP ofrecen a los consumidores (es decir, Spam musical o Contenido engañoso).
- El uso de bots digitales automatizados, u otros medios, direccionados a hacer click en los enlaces de generación de pagos, simulando ser consumidores (es decir, Click Fraud) y produciendo ingresos no naturales y, por tanto, fraudulentos.
- La subida de música deliberadamente distorsionada, canciones vacías, o con cualesquiera otras características defectuosas, con el fin de obtener beneficios ilegítimos, infringiendo así nuestros Términos de Uso o nuestros acuerdos con los DSP.
- Cualquier uso de medios, ya sean manuales o automatizados, bots o cualesquiera otros, con la intención de obtener streams fraudulentos y monetizar contenido en los DSP, en aquellos casos en que esto contradiga las políticas propias de los DSP.
- Cualquier uso de medios, ya sean manuales o automatizados, bots o cualesquiera otros, a través de los MDFS, con el objeto de monetizar contenido propio de manera ilícita.

Royalties (Regalías): Ganancias económicas que corresponden a los legítimos titulares de derechos de propiedad intelectual. A efectos de esta Política, diferenciaremos entre 'Royalties

legítimas', que son el resultado de la explotación lícita y real de un contenido, y 'Royalties ilegítimas', resultado de una explotación fraudulenta de un contenido, generando por tanto unos beneficios ilícitos.

Strike: Penalización aplicable a cualquier Cuenta de Usuario que infrinja lo dispuesto en la presente Política. Están separados en tres niveles (Nivel 1, Nivel 2 y Nivel 3), que serán aplicados gradualmente, y de forma acumulativa. No obstante, según el grado de gravedad de la infracción, la máxima penalización podrá resultar aplicable de manera directa.

3. POLÍTICA ANTI-FRAUDE

El fraude, en todas sus formas y extensión, es inaceptable para Nosotros. Esto es así porque cuando se produce un fraude:

- No solo nos ocasiona pérdidas económicas a Nosotros y a los DSP, sino también a los creadores de contenido, al dañar sus derechos de autor y su reputación. Además, el fraude hace que se reduzca el conjunto de royalties que los DSP ponen a disposición de los creadores de contenido.

- Puede tener una gran repercusión en nuestra reputación y en los contratos que suscribimos con los DSP y, por consiguiente, en otros Usuarios Finales que utilizan nuestros Servicios.

OBJETIVO:

El objetivo específico de la política, es evitar y, si es preciso, eliminar el uso fraudulento de nuestros Servicios. Por todo ello, cualquier indicio de fraude se investigará rigurosamente y se tratará de manera firme y controlada.

3.1 ¿Qué están haciendo los DSP al respecto?

La mayoría de los DSP utilizan tanto a personas como algoritmos para escanear su catálogo y así evitar posibles fraudes o el uso no autorizado de sus servicios. Una vez que han identificado la emisión fraudulenta, eliminan el contenido y nos informan sobre el caso, reservándose el derecho de deducir de futuros pagos aquellas cantidades generadas a partir de actividades sospechosas.

3.2 ¿Qué estamos haciendo al respecto?

Actuamos proactivamente en los siguientes ámbitos:

- Monitorizamos automáticamente los datos históricos de ventas para contrastarlos con otra información como por ejemplo perfiles de artistas, información del Usuario Final, redes sociales, etc., para detectar posibles actividades irregulares.

- Todo nuestro fondo de catálogo y todas las pistas nuevas incorporan huellas digitales y se contrastan con varias bases de datos para evitar una subida múltiple de la misma canción, así como el “ruido blanco”, las “canciones vacías”, la subida de materiales ya protegidos por derechos de autor y, en general, cualquier actividad no autorizada.

- Nuestros procesos de Control de Calidad (QC) están diseñados para rastrear el uso de metadatos que puedan ser engañosos y se traduzcan en Spam musical, Contenido engañoso o cualquier otra actividad no autorizada.

3.3 ¿Cómo actuamos ante un posible fraude?

- En caso de que detectemos o tengamos sospechas de cualquier actividad no autorizada (incluidas reproducciones generadas por bots, Click Fraud, Spam musical, el uso abusivo de MDFS, etc.) en una Cuenta de Usuario especifica, avisaremos al Usuario Final a través del sistema de Política de Strikes, que en última instancia podrá ocasionar el bloqueo de la cuenta implicada.

- Bloquearemos y retendremos de cualquier Cuenta de Usuario los ingresos derivados de un contenido que estimemos, según nuestro exclusivo criterio, infractor de los Términos de Uso.

3.3.1 Medidas para detección de fraude

Se podrán implementar las siguientes medidas, con el fin de mitigar alguna actividad sospechosa.

3.3.1.1 Análisis de Comportamiento

La detección de fraude es un componente crucial en la política antifraude, por ello, se implementarán algunas detecciones así:

- Se implementarán algoritmos avanzados que analicen el comportamiento de los usuarios finales en la plataforma.
- Se buscarán patrones de comportamiento automatizado, como clics fuera de lo común, interacciones predecibles y actividades repetitivas que generen sospecha.

3.3.1.2 Análisis de Huellas Digitales del Dispositivo:

De ser necesario, se recopilarán y analizarán las huellas digitales para contrastar con varias bases de datos para evitar una subida múltiple de la misma canción, así como el “ruido blanco”, las “canciones vacías”, la subida de materiales ya protegidos por derechos de autor y, en general, cualquier actividad no autorizada.

3.3.1.3 Monitoreo de Frecuencia de Acciones:

Podrá a criterio propio, establecer límites de frecuencia para ciertas acciones, como clics o impresiones, durante un período determinado, las actividades que superen estos límites podrían ser indicativas de un comportamiento automatizado y desencadenarán alertas para su revisión.

3.3.1.4 Integración con Listas Negras de Bots Conocidos:

Se integrará la plataforma con listas negras de bots conocidos y patrones de comportamiento asociados con actividades fraudulentas, regularmente, se actualizarán estas listas para adaptarse a nuevas amenazas y tácticas de bots.

3.3.1.5 Colaboración con Proveedores de Servicios Antifraude:

Se podrá establecer asociaciones con proveedores especializados en servicios antifraude que ofrezcan soluciones específicas para la detección de bots, la colaboración con expertos en la industria puede aportar conocimientos valiosos y herramientas adicionales.

3.4 Consecuencias del uso fraudulento de nuestra Plataforma y Servicios

- Si consideramos que un Usuario Final está incumpliendo los Términos de Uso, tendremos derecho a rescindir, unilateralmente, la relación contractual.

- Aquellas cantidades adeudadas a un Usuario Final por parte de cualquier DSP por un uso fraudulento o no autorizado de su servicio podrán ser recuperadas mediante la deducción de dichos importes de los pagos futuros debidos a dicho Usuario Final.

- En caso de que se determine que las actividades fraudulentas y/o ilícitas derivan de las acciones del Usuario Final, cualquier gasto en el que pudiéramos incurrir Nosotros o nuestros proveedores a este respecto (incluidos honorarios y gastos legales) puede ser descontado de cualquier pago futuro debido al Usuario Final, quien será considerado responsable por dichos gastos.

4. SEVERIDAD, POLÍTICA DE STRIKES Y BLOQUEO DE CUENTAS

4.1 Severidad

Durante nuestro proceso de control de calidad y el proceso de confirmación de ventas o a través de notificaciones recibidas por parte de los DSP o un tercero, podemos detectar problemas relacionados con cuentas o contenidos fraudulentos.

Una vez que se ha detectado un contenido o Cuenta fraudulentos, ello dará como resultado la aplicación de un strike y, en los casos más severos, el bloqueo directo de la cuenta implicada. Categorizamos el fraude según sus características y severidad en 4 niveles diferentes, a saber:

- F0: Problemas relacionados con una Cuenta de Usuario.
- F1: Problemas relacionados con el Click Fraud, Contenido engañoso, Spam Musical y los Streamings artificiales.
- F2: Problemas relacionados con la infracción de derechos de Propiedad Intelectual.
- F3: Problemas relacionados con el uso abusivo de los MDFS.

F0: Problemas relacionados con una Cuenta de Usuario
Concretamente, de forma no exhaustiva y a efectos de esta Política, categorizamos como F0 los siguientes supuestos:

- Un perfil de Cuenta de Usuario contiene información falsa, incorrecta o contenido no autorizado que pertenece a un tercero.
- Una actividad de IP irregular e incoherente respecto al país de origen declarado en la Cuenta de Usuario.
- En caso de que un Usuario Final sea interpelado para enviarnos determinada documentación, envíe documentos claramente falsos, o sospechosos, con una intención de engañar y burlar el control.
- Cuando encontremos señales de que un Usuario Final trata deliberadamente de evitar su identificación, la validación de su identidad o su dirección.
- Cuando un Usuario Final genere royalties sin haber antes detallado sus datos personales en la sección ‘Perfil’ del apartado ‘Mi Cuenta’.

F1: Actividades relacionadas con Click Fraud, Misleading, Spam Musical y/o Streaming artificial

Concretamente, de forma no exhaustiva y a efectos de esta Política, categorizamos como F1 los siguientes supuestos:

- Una cuenta que incluya lanzamientos de artistas desconocidos que generen una cantidad muy elevada de reproducciones o visitas y, por consiguiente, muchos ingresos en un corto

período de tiempo sin una base mínima de seguidores, oyentes o espectadores que la respalden (Click Fraud).

- Cualquier aumento repentino e injustificado en las ventas sin que existan números de visitas del perfil o redes sociales en respaldo de dicho aumento.

- Cualquier intento de aprovecharse de la fama y reconocimiento de un artista reconocido, de manera que se utilice su nombre o el título de sus canciones de forma no autorizada para atraer a un potencial consumidor (Contenido engañoso).

- La contratación de servicios de crecimiento de Streamings o Followers de cara a generar popularidad y beneficios artificiales.

F2: Infracciones de Copyright y/o derechos de Propiedad Intelectual o de Marca.
Concretamente, de forma no exhaustiva y a efectos de esta Política, categorizamos como F2 los siguientes supuestos:

- Siempre que se confirme la suplantación de la identidad de cualquier artista, compañía discográfica, etc., así como el uso no autorizado de sus marcas o signos distintivos, títulos de canciones, álbumes, etc.

- La publicación de un contenido protegido por derechos de autor de un tercero, sin haber éste otorgado permisos de publicación al Usuario Final.

- En caso de recibir una notificación por una posible infracción relativa al contenido que se envió a un DSP, por parte del propio DSP o de cualquier tercero.

- En caso de recibir una reclamación por infracción directa por parte del titular de los derechos de autor o su representante.

F3: Supuestos de uso abusivo del MDFS
Concretamente, de forma no exhaustiva y a efectos de esta Política, categorizamos como F3 los siguientes supuestos:

- La inserción de un contenido original propio, dentro o junto con el contenido sobre el que un tercero ostenta los derechos de propiedad intelectual, con el objeto de aprovecharse de la popularidad de este último para obtener mayores beneficios.

- La obtención de streams o visitas artificiales en utilización abusiva del MDFS (por ejemplo, el uso de bots para generar reproducciones artificiales de un contenido monetizado).

- Cualquier aumento repentino en las ventas relacionadas al MDFS, sin una consistencia

histórica apropiada o razón plausible que lo respalde.

En caso de que detectemos alguna de estas actividades fraudulentas por parte del contenido o las acciones de una Cuenta de Usuario, éste recibirá una notificación indicando que hemos detectado una posible infracción e informando acerca de sus consecuencias, descritos a continuación en nuestra Política de strikes.

4.2 Política de strikes

En caso de que detectemos un caso de F1, F2 o F3 en una Cuenta de Usuario, un strike será aplicado a la misma y algunas acciones adicionales por parte del Usuario Final podrán ser requeridas, tales como:

- Completar la información en el apartado 'Mi cuenta' de la plataforma.

- Enviarnos una copia de un documento identificativo oficial (Pasaporte o Documento nacional de identidad).

- En la mayoría de los casos también requerimos perfiles de artista en redes sociales, links de páginas web, así como cualquier otra información acerca del artista para contrastarlo con los datos de ventas.

Tras notificar al Usuario Final de la aplicación del strike y requerir que presente documentación o información adicional:

- Si este ignora deliberadamente nuestra notificación,
- Rechaza proveer o no puede proveer la información/documentación requerida en el plazo de 5 días laborables (a contar desde la fecha de notificación) o,
- Se confirma la actividad fraudulenta, el strike será efectivamente aplicado a la Cuenta de Usuario, lo que tendrá las siguientes consecuencias:

STRIKE 1:

- Se informa al Usuario Final.
- Se da de baja el contenido implicado.
- Aviso de retraso en el pago en el 2o Strike y de bloqueo permanente de cuenta en el 3er Strike.

STRIKE 2:

- Se informa al Usuario Final.
- Se da de baja el contenido implicado.
- Retraso en el pago de royalties: cualquier requerimiento de pago de royalties será

procesado con un retraso inducido de tres meses contando desde la fecha en que el mismo es solicitado.
- Aviso de que la cuenta será permanentemente bloqueada en el 3er Strike y los royalties guardados como depósito (o 'escrow').

STRIKE 3
- Se informa al Usuario Final.
- La cuenta quedará permanentemente bloqueada.
- Se dará de baja tanto el contenido implicado como el resto del catálogo del Usuario Final infractor.
- Las Royalties legítimas se guardarán como depósito (o 'escrow') durante un mínimo de 24 meses y un máximo de 5 años, en consonancia con las políticas de los DSP y el Código Civil español. Las Royalties ilegítimas se devolverán a los DSP.

4.3 Política de Bloqueo de Cuentas

En caso de que un Usuario Final infrinja repetidamente nuestros Términos de Uso, la presente Política o los acuerdos que tenemos con los DSP, podremos proceder a bloquear su Cuenta de Usuario.

Esto tiene las siguientes consecuencias:
- Podremos rescindir la relación contractual con el Usuario Final.
- Se dará de baja todo el catálogo subido por el Usuario Final.
- Las cuentas bloqueadas no podrán acceder a la plataforma y, por tanto, no podrán beneficiarse de nuestros servicios.
- Las Royalties legítimas se retendrán como depósito (o 'escrow') durante un mínimo de 24 meses, y un máximo de 5 años, en consonancia con las políticas de los DSP y el Código Civil español, o bien hasta que las partes hayan solucionado la disputa.
- En el contexto de una disputa, las partes implicadas deberán informarnos acerca del resultado de la misma, tras lo que determinaremos qué cantidades se les deben devolver, incluidos los gastos incurridos o las reclamaciones económicas, las sanciones o las compensaciones establecidas legalmente. Una vez que este proceso haya concluido y haya transcurrido el período de depósito (o 'escrow'), los fondos existentes se liberarán y se transferirán al Usuario Final en caso de ser reclamados.

5. RETENCIÓN DE ROYALTIES (‘ESCROW’) PARA CUENTAS BLOQUEADAS.

Aquellas ganancias económicas, o Royalties, de una Cuenta de Usuario, que estén en conexión con contenidos que, a nuestra discreción, consideremos que están involucrados en cualquier tipo de actividad que infrinja nuestros Términos de Uso, serán retenidas como depósito (o ‘escrow’). Esta retención se prolongará por un mínimo de 24 meses y un máximo de 5 años, en consonancia con las políticas de los DSP y el Código Civil español, o bien hasta que la disputa entre las partes se solvente, y se prevé como respuesta ante los siguientes posibles escenarios:

5.1 Devolución de Royalties ilegítimas:

Tras recibir una reclamación por parte de un DSP, solicitando la devolución de royalties, en los casos en que este considere que las mismas fueron generadas a partir de actividades fraudulentas. Es importante respetar el período de 24 meses dado que, contractualmente, los DSP tienen el derecho de reclamar royalties durante ese plazo.

5.2 Devolución de Royalties legítimas:

El legítimo titular de los derechos de autor nos reclama el ingreso de aquellas cantidades retenidas.

6. RETIRO DEL CONTENIDO

Iniciaremos la baja del contenido siempre que se confirme una infracción por parte de cualquier Cuenta de Usuario, es decir, de todo contenido implicado en casos de F0, F1, F2 y/o F3.

En cuanto a los casos de F3, y aunque únicamente parte del contenido del Usuario Final esté relacionado con el fraude, podremos a nuestra discreción dar de baja todo su catálogo.

Conviene tener en cuenta también que cualquier contenido puede señalarse como sospechoso por parte de los DSP y éstos pueden retirarlo de su servicio según su exclusivo criterio.

7. REVISIÓN PERIÓDICA

DINASTIA MARKET INC & DINASTIA MARKET LLC como Distribuidor de música digital, se compromete a llevar a cabo revisiones sistemáticas y periódicas de esta política antifraude para asegurar su relevancia y efectividad en el tiempo.

Estas revisiones se llevarán a cabo al menos anualmente, aunque podrían realizarse con mayor frecuencia si se identifican cambios significativos en el entorno empresarial, tecnológico o normativo que puedan afectar la eficacia de la política.

Durante estas revisiones, se considerarán los siguientes aspectos:

7.1 Evaluación de Riesgos Actuales

Se realizará una revisión exhaustiva de los riesgos actuales de fraude que podrían afectar directamente a DINASTIA MARKET INC como a terceros. Esto incluirá la identificación de nuevas amenazas y vulnerabilidades, así como la evaluación de la efectividad de las medidas de control existentes.

7.2 Actualización Normativa

La política será revisada a la luz de cambios en las leyes, regulaciones y estándares de la industria relacionados con la prevención y detección de fraudes. Se realizarán ajustes necesarios para garantizar el cumplimiento continuo con todas las normativas aplicables.

7.3 Retroalimentación de Incidentes

Se revisarán los incidentes anteriores, si los hubiera, para extraer variantes y mejorar las estrategias de prevención y detección. La retroalimentación de incidentes también puede ayudar a identificar nuevas tácticas de fraude o patrones de comportamiento.

7.4 Mejoras Tecnológicas

Se evaluarán las tecnologías y herramientas utilizadas para prevenir y detectar. Si hay avances tecnológicos significativos o nuevas soluciones disponibles, se considerará su implementación para mejorar la seguridad.

7.5 Cambios

Cualquier cambio en la arquitectura, funcionalidad o características, será tenido en cuenta durante la revisión. Se ajustarán las políticas según sea necesario para abordar cualquier cambio que pueda afectar la seguridad.

7.6 Participación de los Terceros

Se recopilará si es necesario, la retroalimentación de terceros usuarios, para obtener perspectivas sobre la eficacia de las políticas antifraude. Esto puede incluir encuestas, reuniones de retroalimentación y revisiones conjuntas.

7.7 Capacitación Continua

Se evaluará la efectividad de los programas de capacitación proporcionados tanto internamente, como a terceros y se realizarán ajustes según sea necesario. La capacitación continuará siendo una parte integral de la estrategia antifraude.

7.8 Comunicación y Divulgación

Cualquier cambio significativo en la política será comunicado de manera clara y oportuna. Se proporcionará orientación adicional de ser requerida y se responderán preguntas para garantizar la comprensión y el cumplimiento continuo.

7.9 Documentación Actualizada

La documentación asociada con la política antifraude que pueda surgir, incluyendo manuales, procedimientos y formularios, será revisada y actualizada según sea necesario para reflejar los cambios realizados en la política.

Estas revisiones periódicas son esenciales para garantizar que la política antifraude, siga siendo efectiva y esté alineada con los estándares más recientes, las mejores prácticas y las necesidades cambiantes de la organización y sus usuarios. La retroalimentación de todas las partes interesadas será bienvenida y se utilizará para mejorar continuamente las medidas de seguridad implementadas.

7.10 REVISIÓN FUTURA

DINASTÍA MARKET INC se compromete a continuar con el ciclo de revisión periódica, adaptando las políticas antifraude según sea necesario. Se programarán futuras revisiones y se asignarán los recursos necesarios para garantizar la efectividad continua de las políticas en la prevención y detección de fraudes.

Con la implementación de estos pasos, se busca cerrar el ciclo de revisión de políticas antifraude de manera integral, asegurando una transición armoniosa, la comprensión generalizada y el compromiso continuo de todas las partes involucradas en la lucha contra el fraude en la organización.