

Contenido

1.	Objetivo.....	3
2.	Alcance.....	3
3.	Principios generales.....	3
3.1.	Uso legítimo del servicio.....	4
3.2.	Responsabilidad sobre el contenido.....	4
3.3.	Prevención desde el diseño.....	4
3.4.	Colaboración activa.....	4
3.5.	Actuación oportuna.....	4
4.	Definiciones.....	4
4.1.	Fraude.....	4
4.2.	Smishing.....	4
4.3.	Phishing.....	5
4.4.	Suplantación.....	5
4.5.	Contenido fraudulento o sospechoso.....	5
4.6.	Cliente o Suscriptor.....	5
4.7.	Usuario final.....	5
5.	Obligaciones del cliente.....	5
5.1.	Uso autorizado de la plataforma.....	5
5.2.	Control sobre el contenido de los mensajes.....	6
5.3.	Prohibición de contenidos fraudulentos o engañosos.....	6
5.4.	Notificación de irregularidades.....	6
5.5.	Colaboración con INALAMBRIA.....	7
5.6.	Control de terceros.....	7
5.7.	Actualización de información.....	7
6.	Controles de prevención de fraude de INALAMBRIA.....	8
6.1.	Validación de clientes.....	8
6.2.	Validación de remitentes, marcas y códigos.....	8
6.3.	Monitoreo de contenido.....	8
6.4.	Análisis de enlaces y dominios.....	8
6.5.	Reglas de bloqueo preventivo.....	8
6.6.	Trazabilidad y auditoría.....	8



6.7.	Gestión de riesgo progresiva	9
7.	Señales de alerta	9
8.	Manejo de incidentes o sospechas de fraude	10
9.	Suspensión preventiva del servicio	10
10.	Reactivación del servicio	11
11.	Responsabilidad del cliente frente a bases de datos y destinatarios	11
12.	Protección de credenciales y accesos.....	12
13.	Cooperación con autoridades y terceros afectados.....	12
14.	Consecuencias del incumplimiento	12
15.	Buenas prácticas recomendadas para clientes	13
15.1.	Antes de enviar una campaña	13
15.2.	Durante el envío.....	13
15.3.	Después del envío.....	13
16.	Canales de reporte.....	13
17.	Actualización de la política.....	14
18.	Aceptación.....	14
19.	Revisión y Mejora Continua.....	14
20.	Anexos.....	14
	Anexo 1. Ejemplos de mensajes de alto riesgo	14
	Anexo 2. Checklist mínimo para campañas con enlaces	15
	Anexo 3. Información mínima sugerida para reportar un incidente.....	15



	Política de Prevención de Fraude	PLT-SIG-SGSI-010 PÚBLICA
		Versión:001
		Fecha de Versión: feb 11.2024
		Actualización: abr 24.2026
		Página 3 de 16

1. Objetivo

INALAMBRIA Internacional S.A.S. ("INALAMBRIA") presta servicios de comunicación empresarial a través de canales digitales como SMS, mensajería instantánea, correo electrónico y otros medios habilitados dentro de sus plataformas.

Dado que estos canales pueden ser utilizados indebidamente por terceros para ejecutar actividades fraudulentas, suplantación, phishing, smishing, envío de enlaces maliciosos, ingeniería social u otras conductas abusivas, INALAMBRIA adopta la presente Política de Prevención de Fraude con el fin de establecer los principios, obligaciones, controles y procedimientos mínimos que deben cumplir sus clientes y usuarios autorizados.

El objetivo principal de esta política es proteger a los usuarios finales, a los clientes, al ecosistema de comunicaciones empresariales, a los operadores, a las entidades regulatorias y a INALAMBRIA frente al uso indebido de los servicios contratados.

2. Alcance

Esta política aplica a todos los clientes, suscriptores, aliados, integradores, proveedores, terceros autorizados y usuarios que utilicen directa o indirectamente los servicios de INALAMBRIA para el envío, procesamiento, automatización, integración, enrutamiento o gestión de comunicaciones empresariales.

Plataformas, APIs, conexiones o canales de comunicación provistos por INALAMBRIA.

La política cubre, entre otros, los siguientes servicios y canales:

- Envío de mensajes SMS empresariales.
- Mensajes transaccionales, promocionales, informativos, de autenticación u OTP.
- Comunicaciones con enlaces, URLs, dominios, archivos, formularios o mecanismos de redirección.
- Integraciones vía API, SMPP, plataformas web, conectores, formularios, cargas masivas o cualquier otro mecanismo habilitado por INALAMBRIA.
- Uso de códigos cortos, remitentes, nombres de marca, campañas, plantillas, bases de datos y contenidos enviados a través de la plataforma.

3. Principios generales

La prevención de fraude en INALAMBRIA se fundamenta en los siguientes principios:



	Política de Prevención de Fraude	PLT-SIG-SGSI-010
		PÚBLICA
		Versión:001
		Fecha de Versión: feb 11.2024
		Actualización: abr 24.2026
		Página 4 de 16

3.1. Uso legítimo del servicio

Los servicios de INALAMBRIA deben utilizarse únicamente para comunicaciones lícitas, autorizadas, transparentes y relacionadas con las actividades legítimas del cliente.

3.2. Responsabilidad sobre el contenido

El cliente es responsable por el contenido de los mensajes que procese a través de INALAMBRIA, incluyendo textos, enlaces, archivos, dominios, redirecciones, números de contacto, llamadas a la acción, remitentes, marcas, campañas y cualquier otro elemento incluido en la comunicación.

3.3. Prevención desde el diseño

Los clientes deben adoptar controles internos para prevenir que sus procesos, usuarios, credenciales, integraciones, bases de datos o campañas sean utilizados para actividades fraudulentas o abusivas.

3.4. Colaboración activa

La prevención de fraude requiere cooperación entre INALAMBRIA, sus clientes, aliados, operadores, autoridades competentes, entidades regulatorias y demás actores del ecosistema.

3.5. Actuación oportuna

Ante señales de fraude, sospecha razonable, abuso, suplantación, uso no autorizado o riesgo para usuarios finales, INALAMBRIA podrá adoptar medidas preventivas, correctivas o restrictivas de manera inmediata.

4. Definiciones

Para efectos de esta política, se tendrán en cuenta las siguientes definiciones:

4.1. Fraude

Cualquier conducta mediante la cual una persona o entidad utilice información falsa, engañosa, manipulada, suplantada o no autorizada para obtener un beneficio indebido, causar daño, inducir a error o afectar a usuarios, clientes, terceros, operadores o a INALAMBRIA.

4.2. Smishing

Modalidad de fraude en la que se utilizan mensajes de texto u otros canales de mensajería para engañar a usuarios finales, normalmente mediante enlaces falsos,



	Política de Prevención de Fraude	PLT-SIG-SGSI-010 PÚBLICA
		Versión:001
		Fecha de Versión: feb 11.2024
		Actualización: abr 24.2026
		Página 5 de 16

suplantación de marcas, solicitudes de información sensible o instrucciones engañosas.

4.3. Phishing

Técnica de suplantación mediante la cual se busca obtener credenciales, información financiera, datos personales, códigos de autenticación, pagos o acceso a sistemas mediante comunicaciones engañosas.

4.4. Suplantación

Uso no autorizado de nombres, marcas, dominios, remitentes, logos, entidades, personas, instituciones o identidades comerciales con el fin de inducir a error a los destinatarios o a terceros.

4.5. Contenido fraudulento o sospechoso

Contenido que, por sus características, estructura, intención, enlaces, lenguaje, urgencia, promesa, origen, destino o comportamiento, pueda estar asociado a fraude, abuso, suplantación, engaño, captación indebida de datos, malware, cobros no autorizados o actividades ilícitas.

4.6. Cliente o Suscriptor

Persona natural o jurídica que contrata, utiliza o accede directa o indirectamente a los servicios de INALAMBRIA.

4.7. Usuario final

Persona destinataria de una comunicación enviada a través de los servicios de INALAMBRIA.

5. Obligaciones del cliente

Todo cliente que utilice los servicios de INALAMBRIA se obliga a cumplir esta Política de Prevención de Fraude y, en particular, a adoptar las siguientes medidas:

5.1. Uso autorizado de la plataforma

El cliente deberá garantizar que la plataforma, API, credenciales, usuarios, conexiones, integraciones y servicios contratados sean utilizados únicamente por personal autorizado y para fines legítimos.

El cliente deberá proteger sus credenciales de acceso, llaves API, usuarios, contraseñas, tokens, certificados, conexiones SMPP o cualquier otro mecanismo de autenticación provisto por INALAMBRIA.



	Política de Prevención de Fraude	PLT-SIG-SGSI-010 PÚBLICA
		Versión:001
		Fecha de Versión: feb 11.2024
		Actualización: abr 24.2026
		Página 6 de 16

5.2. Control sobre el contenido de los mensajes

El cliente deberá mantener controles de prevención de fraude sobre el contenido de los mensajes que procese a través de INALAMBRIA, incluyendo, entre otros:

- Validación del origen de las campañas.
- Revisión del texto de los mensajes.
- Validación de enlaces incluidos en las comunicaciones.
- Control sobre dominios, acortadores, redirecciones o formularios.
- Aprobación interna de campañas sensibles.
- Revisión de mensajes relacionados con pagos, autenticación, claves, códigos OTP, datos financieros, datos personales o información sensible.

5.3. Prohibición de contenidos fraudulentos o engañosos

El cliente no podrá utilizar los servicios de INALAMBRIA para enviar, procesar, facilitar o permitir comunicaciones que:

- Suplanten marcas, entidades públicas, entidades financieras, comercios, operadores, plataformas digitales o cualquier tercero.
- Induzcan al usuario final a entregar claves, códigos OTP, datos financieros, datos personales, credenciales o información sensible bajo engaño.
- Incluyan enlaces maliciosos, dominios falsos, páginas clonadas, malware, formularios fraudulentos o redirecciones sospechosas.
- Promuevan actividades ilícitas, engañosas, abusivas o no autorizadas.
- Utilicen urgencia, amenazas, premios falsos, bloqueos inexistentes, cobros falsos o alertas engañosas para manipular al usuario final.
- Se envíen sin autorización legal, contractual o comercial suficiente.

5.4. Notificación de irregularidades

El cliente deberá notificar de manera inmediata a INALAMBRIA cualquier irregularidad, sospecha de fraude, incidente, acceso no autorizado, uso indebido, vulneración de credenciales, compromiso de sistemas, suplantación o hecho de fraude detectado en su organización que pueda afectar el cumplimiento del contrato o el uso adecuado de los servicios.

La notificación deberá incluir, en la medida en que esté disponible:

- Fecha y hora aproximada del incidente.
- Descripción de los hechos.
- Servicios, campañas, usuarios, credenciales o integraciones involucradas.



	Política de Prevención de Fraude	PLT-SIG-SGSI-010 PÚBLICA
		Versión:001
		Fecha de Versión: feb 11.2024
		Actualización: abr 24.2026
		Página 7 de 16

- Mensajes, enlaces, remitentes o bases de datos afectados.
- Medidas adoptadas por el cliente.
- Persona de contacto para la coordinación del caso.

5.5. Colaboración con INALAMBRIA

El cliente deberá prestar colaboración al Oficial de Prevención de Fraude, Auditor Interno o equipo designado por INALAMBRIA para analizar si los procedimientos, procesos, actividades, campañas, integraciones o controles del cliente pueden afectar el cumplimiento del contrato o generar riesgos de fraude.

Dicha colaboración podrá incluir, entre otras acciones:

- Entregar información razonable sobre campañas, procesos o integraciones.
- Explicar el origen y propósito de determinados mensajes.
- Aportar evidencias sobre la legitimidad de una campaña.
- Confirmar la titularidad o autorización de uso de marcas, dominios, remitentes o códigos.
- Implementar ajustes o controles solicitados por INALAMBRIA.
- Suspender temporalmente campañas, accesos, usuarios o integraciones cuando exista riesgo relevante.

5.6. Control de terceros

Cuando el cliente permita que terceros, proveedores, agencias, aliados, integradores o usuarios externos utilicen los servicios de INALAMBRIA en su nombre, será responsable de asegurar que dichos terceros cumplan esta política.

El cliente responderá por el uso de la plataforma realizado mediante sus credenciales, accesos, cuentas, integraciones o servicios contratados.

5.7. Actualización de información

El cliente deberá mantener actualizada la información relacionada con su identidad, datos de contacto, responsables técnicos, responsables administrativos, dominios autorizados, remitentes, marcas, casos de uso y demás información solicitada por INALAMBRIA para fines de control, trazabilidad, seguridad y prevención de fraude.



	Política de Prevención de Fraude	PLT-SIG-SGSI-010 PÚBLICA
		Versión:001
		Fecha de Versión: feb 11.2024
		Actualización: abr 24.2026
		Página 8 de 16

6. Controles de prevención de fraude de INALAMBRIA

INALAMBRIA podrá implementar controles manuales, automáticos, tecnológicos, operativos, contractuales y de monitoreo para prevenir, detectar, analizar y mitigar riesgos de fraude en sus plataformas y servicios.

Estos controles podrán incluir, entre otros:

6.1. Validación de clientes

INALAMBRIA podrá solicitar información al cliente para validar su identidad, actividad económica, legitimidad comercial, casos de uso, autorización de marca, propósito del servicio, responsable contractual, responsable técnico y demás elementos necesarios para evaluar el riesgo asociado a la prestación del servicio.

6.2. Validación de remitentes, marcas y códigos

INALAMBRIA podrá requerir evidencia de autorización para el uso de marcas, nombres comerciales, remitentes, códigos cortos, dominios, URLs o cualquier identificador utilizado en una comunicación.

6.3. Monitoreo de contenido

INALAMBRIA podrá monitorear, analizar o bloquear contenido que presente señales de fraude, abuso, suplantación, enlaces sospechosos, patrones anómalos, uso indebido de marcas, lenguaje engañoso o cualquier otro indicador de riesgo.

6.4. Análisis de enlaces y dominios

INALAMBRIA podrá revisar enlaces, URLs, dominios, redirecciones, acortadores o páginas asociadas a los mensajes procesados, con el fin de identificar riesgos de phishing, smishing, malware, suplantación o captación indebida de información.

6.5. Reglas de bloqueo preventivo

INALAMBRIA podrá bloquear preventivamente mensajes, campañas, remitentes, URLs, dominios, clientes, usuarios, credenciales, integraciones o conexiones cuando existan señales razonables de fraude, abuso, riesgo reputacional, riesgo operativo, afectación a usuarios finales o incumplimiento de esta política.

6.6. Trazabilidad y auditoría

INALAMBRIA podrá conservar registros técnicos, transaccionales, operativos y de auditoría relacionados con el uso de sus servicios, de acuerdo con la legislación aplicable, las obligaciones contractuales y sus políticas internas de seguridad de la información.



	Política de Prevención de Fraude	PLT-SIG-SGSI-010 PÚBLICA
		Versión:001
		Fecha de Versión: feb 11.2024
		Actualización: abr 24.2026
		Página 9 de 16

6.7. Gestión de riesgo progresiva

INALAMBRIA podrá aplicar controles diferenciales según el nivel de conocimiento, historial, comportamiento, volumen, tipo de tráfico, criticidad del caso de uso, madurez operativa y riesgo asociado al cliente o campaña.

Esto significa que ciertas funcionalidades, volúmenes, rutas, permisos, integraciones o capacidades podrán ser habilitadas, restringidas o condicionadas de manera progresiva según el perfil de riesgo del cliente.

7. Señales de alerta

Se consideran señales de alerta, entre otras, las siguientes situaciones:

- Cambios repentinos o inusuales en el volumen de mensajes.
- Envío de mensajes con enlaces no informados o no autorizados.
- Uso de acortadores de URL sin justificación o trazabilidad.
- Mensajes que simulan ser de bancos, entidades públicas, operadores, comercios, billeteras digitales o plataformas reconocidas sin autorización verificable.
- Mensajes que solicitan claves, códigos OTP, datos personales, datos financieros o pagos bajo presión o urgencia.
- Campañas con múltiples dominios, redirecciones o páginas de destino cambiantes.
- Intentos de evadir controles de contenido, filtros, bloqueos o validaciones.
- Uso de lenguaje asociado a premios falsos, bloqueos de cuentas, multas, embargos, retenciones, pagos urgentes o beneficios inexistentes.
- Reclamos de usuarios finales, operadores, autoridades, entidades afectadas o terceros sobre posible fraude.
- Accesos inusuales a la plataforma, cambios no autorizados en usuarios o uso anómalo de credenciales.
- Reutilización de patrones, textos, dominios o estructuras previamente asociados con fraude.

La existencia de una señal de alerta no implica necesariamente la ocurrencia de fraude, pero habilita a INALAMBRIA a realizar verificaciones, solicitar información, aplicar medidas preventivas o suspender temporalmente el procesamiento de tráfico relacionado.



	Política de Prevención de Fraude	PLT-SIG-SGSI-010 PÚBLICA
		Versión:001
		Fecha de Versión: feb 11.2024
		Actualización: abr 24.2026
		Página 10 de 16

8. Manejo de incidentes o sospechas de fraude

Cuando INALAMBRIA detecte o reciba información sobre una posible irregularidad, abuso, fraude o incumplimiento de esta política, podrá adelantar una o varias de las siguientes acciones:

- 1) Analizar el contenido, campaña, cliente, usuario, conexión, URL, dominio, remitente o patrón involucrado.
- 2) Solicitar información adicional al cliente.
- 3) Suspender preventivamente mensajes, campañas, usuarios, credenciales, integraciones o servicios relacionados.
- 4) Bloquear URLs, dominios, remitentes, textos, patrones o destinatarios específicos.
- 5) Requerir al cliente ajustes en sus procesos, controles, contenidos o integraciones.
- 6) Escalar el caso internamente al Oficial de Prevención de Fraude, Auditor Interno, equipo jurídico, equipo de seguridad o área responsable.
- 7) Informar a operadores, aliados, entidades afectadas, autoridades competentes o entidades regulatorias cuando corresponda.
- 8) Adoptar medidas contractuales, comerciales, técnicas u operativas frente al cliente o tercero involucrado.

9. Suspensión preventiva del servicio

INALAMBRIA podrá suspender total o parcialmente el servicio, sin que ello constituya incumplimiento contractual, cuando exista una sospecha razonable de fraude, abuso, uso indebido, afectación a usuarios finales, riesgo para el ecosistema, requerimiento de autoridad competente, incumplimiento de esta política o falta de colaboración del cliente.

La suspensión podrá aplicar sobre:

- Una campaña específica.
- Un remitente.
- Un dominio o URL.
- Un usuario de plataforma.
- Una llave API, conexión SMPP, token o credencial.
- Una cuenta completa.
- Un canal, ruta o servicio específico.



	Política de Prevención de Fraude	PLT-SIG-SGSI-010
		PÚBLICA
		Versión:001
		Fecha de Versión: feb 11.2024
		Actualización: abr 24.2026
		Página 11 de 16

Cuando las circunstancias lo permitan, INALAMBRIA informará al cliente sobre la medida adoptada y las acciones requeridas para evaluar la reactivación del servicio.

10. Reactivación del servicio

La reactivación total o parcial del servicio estará sujeta a la evaluación de INALAMBRIA y podrá requerir, entre otros:

- Explicación satisfactoria del incidente.
- Corrección de la causa raíz.
- Cambio de credenciales, usuarios, tokens o mecanismos de acceso.
- Eliminación o modificación de contenidos, enlaces, dominios o campañas.
- Evidencia de autorización para uso de marca, remitente, código o dominio.
- Implementación de controles adicionales por parte del cliente.
- Compromiso formal de cumplimiento de esta política.

INALAMBRIA podrá negar la reactivación cuando considere que persiste un riesgo relevante para usuarios finales, operadores, aliados, autoridades, terceros, el ecosistema o la propia compañía.

11. Responsabilidad del cliente frente a bases de datos y destinatarios

El cliente declara y garantiza que cuenta con las autorizaciones necesarias para contactar a los destinatarios de sus comunicaciones, así como para tratar sus datos personales conforme a la normativa aplicable.

El cliente deberá mantener mecanismos adecuados para:

- Gestionar autorizaciones de contacto.
- Atender solicitudes de baja o exclusión.
- Evitar el envío a destinatarios no autorizados.
- Respetar restricciones legales, regulatorias o contractuales aplicables.
- Evitar prácticas abusivas, engañosas o invasivas.

El uso de bases de datos no autorizadas, compradas irregularmente, obtenidas sin consentimiento o utilizadas para fines distintos a los autorizados podrá ser considerado incumplimiento de esta política.



	Política de Prevención de Fraude	PLT-SIG-SGSI-010 PÚBLICA
		Versión:001
		Fecha de Versión: feb 11.2024
		Actualización: abr 24.2026
		Página 12 de 16

12. Protección de credenciales y accesos

El cliente deberá adoptar medidas razonables de seguridad para proteger sus accesos a los servicios de INALAMBRIA.

Como mínimo, el cliente deberá:

- Asignar usuarios individuales y evitar usuarios compartidos cuando la plataforma lo permita.
- Revocar accesos de empleados, proveedores o terceros que ya no estén autorizados.
- Proteger contraseñas, tokens, llaves API y credenciales técnicas.
- Notificar de inmediato cualquier pérdida, filtración, exposición o uso no autorizado de credenciales.
- Limitar el acceso a personal que realmente requiera operar el servicio.
- Implementar controles internos de aprobación para campañas sensibles.

Todo uso realizado mediante credenciales del cliente se presumirá efectuado por el cliente o por personas autorizadas por este, salvo evidencia en contrario.

13. Cooperación con autoridades y terceros afectados

INALAMBRIA podrá colaborar con autoridades competentes, entidades regulatorias, operadores, clientes afectados, marcas suplantadas, entidades financieras, comercios, proveedores tecnológicos o terceros relevantes cuando se identifiquen eventos de fraude, sospecha de fraude, abuso o uso indebido de sus servicios.

Dicha colaboración se realizará dentro del marco legal aplicable, los contratos vigentes, las políticas internas de seguridad de la información y las obligaciones de confidencialidad correspondientes.

14. Consecuencias del incumplimiento

El incumplimiento de esta política podrá dar lugar a una o varias de las siguientes medidas:

- Solicitud de información o aclaración al cliente.
- Bloqueo o rechazo de mensajes específicos.
- Suspensión de campañas, usuarios, credenciales, rutas, integraciones o servicios.
- Restricción de funcionalidades.



	Política de Prevención de Fraude	PLT-SIG-SGSI-010 PÚBLICA
		Versión:001
		Fecha de Versión: feb 11.2024
		Actualización: abr 24.2026
		Página 13 de 16

- Terminación del contrato o de la relación comercial.
- Reporte a autoridades competentes cuando corresponda.
- Reclamación de perjuicios, costos, sanciones, multas, daños reputacionales o afectaciones derivadas del incumplimiento.

Estas medidas podrán aplicarse sin perjuicio de las demás acciones legales, contractuales, regulatorias o comerciales a las que haya lugar.

15. Buenas prácticas recomendadas para clientes

INALAMBRIA recomienda a sus clientes adoptar, como mínimo, las siguientes buenas prácticas:

15.1. Antes de enviar una campaña

- Validar que el caso de uso sea legítimo y esté autorizado.
- Revisar cuidadosamente el texto del mensaje.
- Confirmar que los enlaces pertenezcan a dominios oficiales o autorizados.
- Evitar acortadores de URL cuando no sean necesarios.
- Verificar que la marca, remitente o código usado corresponda al cliente.
- Revisar si el mensaje puede ser confundido con una comunicación fraudulenta.
- Validar que la base de datos cuente con autorización suficiente.

15.2. Durante el envío

- Monitorear volúmenes y comportamiento de la campaña.
- Estar atento a quejas, alertas o reportes de usuarios.
- Suspender inmediatamente cualquier campaña que genere sospechas.
- Informar a INALAMBRIA cualquier comportamiento inusual.

15.3. Después del envío

- Revisar métricas, reclamos, bloqueos o alertas.
- Documentar aprendizajes o incidentes.
- Ajustar procesos internos para reducir riesgos futuros.
- Mantener evidencia de autorizaciones, aprobaciones y controles aplicados.

16. Canales de reporte

Los clientes deberán reportar cualquier irregularidad, sospecha de fraude, incidente de seguridad, suplantación, uso indebido o evento relacionado con esta política a



	Política de Prevención de Fraude	PLT-SIG-SGSI-010
		PÚBLICA
		Versión:001
		Fecha de Versión: feb 11.2024
		Actualización: abr 24.2026
		Página 14 de 16

través de los canales oficiales de atención, soporte, gestión de cuenta o contacto contractual definidos por INALAMBRIA.

El reporte oportuno es fundamental para mitigar riesgos, proteger a los usuarios finales y reducir el impacto de posibles incidentes.

17. Actualización de la política

INALAMBRIA podrá actualizar esta Política de Prevención de Fraude en cualquier momento para reflejar cambios regulatorios, tecnológicos, operativos, contractuales, comerciales o de riesgo.

La versión vigente será la publicada o comunicada por INALAMBRIA a sus clientes a través de sus canales oficiales.

18. Aceptación

El uso de los servicios de INALAMBRIA implica el conocimiento, aceptación y cumplimiento de esta Política de Prevención de Fraude.

El cliente reconoce que la prevención de fraude es una obligación permanente y compartida, y que el cumplimiento de esta política es una condición esencial para el uso adecuado, seguro y responsable de los servicios contratados.

19. Revisión y Mejora Continua

Esta política será revisada:

- Al menos una vez al año.
- Ante incidentes relevantes de fraude.
- Cuando cambie el marco regulatorio o el modelo de negocio.

20. Anexos

Anexo 1. Ejemplos de mensajes de alto riesgo

Los siguientes ejemplos son ilustrativos y no limitan la capacidad de INALAMBRIA para identificar otros patrones de riesgo:

- "Su cuenta será bloqueada. Ingrese aquí para evitar la suspensión."
- "Tiene una multa pendiente. Pague de inmediato en este enlace."
- "Reclame su premio ingresando sus datos bancarios."
- "Actualice su clave para evitar el cierre de su cuenta."



	Política de Prevención de Fraude	PLT-SIG-SGSI-010 PÚBLICA
		Versión:001
		Fecha de Versión: feb 11.2024
		Actualización: abr 24.2026
		Página 15 de 16

- "Confirme su código de seguridad en el siguiente formulario."
- "Su paquete está retenido. Realice el pago aquí."
- "Su entidad financiera requiere validación urgente."

Estos patrones suelen combinar urgencia, amenaza, promesa, suplantación o enlaces sospechosos. Por tanto, deben ser revisados con especial cuidado antes de su envío.

Anexo 2. Checklist mínimo para campañas con enlaces

Antes de enviar mensajes que contengan enlaces, el cliente debería validar:

1. El dominio pertenece al cliente o está formalmente autorizado.
2. La página de destino corresponde al propósito informado en el mensaje.
3. No se solicitan datos sensibles de forma innecesaria o engañosa.
4. No hay redirecciones ocultas, múltiples o no justificadas.
5. El texto del mensaje identifica claramente al remitente.
6. La campaña fue aprobada por el área responsable del cliente.
7. El enlace no imita dominios de terceros ni marcas ajenas.
8. La página de destino cuenta con controles básicos de seguridad.
9. El mensaje no puede inducir a error al usuario final.
10. Existe trazabilidad interna sobre quién creó, aprobó y ejecutó la campaña.

Anexo 3. Información mínima sugerida para reportar un incidente

Cuando el cliente reporte una sospecha o evento de fraude, se recomienda incluir:

- Nombre del cliente.
- Nombre y datos de contacto del responsable del reporte.
- Fecha y hora aproximada del incidente.
- Descripción de lo ocurrido.
- Canal afectado.
- Mensajes involucrados.
- URLs, dominios o remitentes asociados.
- Usuarios, credenciales o integraciones involucradas.
- Volumen aproximado de mensajes afectados.
- Evidencias disponibles.
- Medidas adoptadas internamente.
- Nivel de urgencia percibido.



Control Documental

Control de cambios			
REV N°	Descripción del cambio	Realizo	Fecha
1	Emisión Primer documento		
2	Revisión sin cambios	Líder de Seguridad de la Información y SIG	Abr.24.2026
3			

Elaboró	Revisó:	Aprobó:
Mile Castaño	Olga Martínez	Carlos Sierra
Subgerente	Líder de Seguridad de la Información y SIG	Gerente



Documento aprobado mediante proceso de autorización digital. No requiere firma física.

