

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

ANEXO 5

REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS

GERENCIA DE SEGURIDAD DE LA INFORMACIÓN

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 1 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

AVISO DE PROPIEDAD

La información aquí contenida es propiedad de **COMCEL S.A.**, por lo tanto, no debe reproducirse, exponerse o discutirse más allá del grupo a quien va dirigida. Al recibir este documento, el Destinatario acuerda no reproducir o hacer esta información disponible en ninguna forma a personas que no estén directamente relacionadas y sean responsables de la evaluación de su contenido.

COMCEL S.A. no aceptará ninguna responsabilidad económica o de cualquier otro tipo que pueda ser resultado del uso que se le dé a la información contenida en este documento, incluyendo, pero no limitándose a, daños directos, especiales o consecuentes. Esta información podrá cambiar o ser actualizada sin previo aviso conforme lo requiera **COMCEL S.A.** Todos los requerimientos, diagramas e información contenida en este documento representan información propietaria y confidencial de **COMCEL S.A.**

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 2 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

OBJETIVO

Establecer los requerimientos mínimos de **Seguridad de la Información y Ciberseguridad** que deberán ser tenidos en cuenta por los proveedores, distribuidores, aliados y/o contratistas que accedan, transporten, intercambien, custodien o almacenen, por cualquier medio, información o tengan acceso a los sistemas informáticos de **COMCEL S.A.** y (en adelante **CLARO COLOMBIA**) y **Hitss Colombia S.A.S.**

ALCANCE

Todo tercero, proveedor, distribuidor, aliado y/o contratista de **CLARO COLOMBIA**, en adelante y para efectos del presente Anexo se denominará “**EL CONTRATISTA**”.

EL CONTRATISTA no deberá interpretar el presente documento como una política propia, manual de seguridad o guía de implementación, puesto que su información se refiere exclusivamente a lineamientos y estándares de seguridad de carácter general, que deberán ser adoptados conforme a las particularidades del servicio prestado a **CLARO COLOMBIA**. Dado que **EL CONTRATISTA** es el único y directo responsable de la operación y aseguramiento de toda su infraestructura, de su información, de los sistemas informáticos, de la información que procesa en nombre de **CLARO COLOMBIA** y de los accesos a los sistemas que este autorizado, por lo cual es responsable de conocer y gestionar los riesgos y amenazas de seguridad que puedan surgir; en este sentido deberá contar con controles, normas políticas y procedimientos internos complementarios a los lineamientos y estándares aquí establecidos, que le aseguren el establecimiento y mantenimiento niveles óptimos de seguridad.

Así mismo **EL CONTRATISTA** es responsable de conocer y asegurar el cumplimiento de sus obligaciones en la Seguridad de Información, según las leyes, normativas y estándares que abarcan tanto la protección de datos personales como la seguridad de los sistemas de información y gobernanza de la seguridad digital, emitidos para la República de Colombia. Entre estos se tienen, sin limitarse a las normas ISO 2700* que se refieren principalmente a la familia de estándares **ISO/IEC 27000**, que se enfocan en la gestión de la seguridad de la información, así como la ley de datos

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 3 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

personales en Colombia, también conocida como la **Ley 1581 de 2012**, sus decretos reglamentarios, y demás normatividad complementaria que la modifique o adicione, así como también las circulares, instrucciones y órdenes emitidas por la Superintendencia de Industria y Comercio, como autoridad nacional de protección de datos personales en Colombia.

Por lo anterior, **EL CONTRATISTA** se compromete a cumplir a cabalidad con este Anexo durante la ejecución del contrato u orden de compra del que hace parte integral.

1. CUMPLIMIENTO NORMATIVO O REGULATORIO

- 1.1. **EL CONTRATISTA** deberá contar con políticas, procedimientos, estándares y/o metodologías de seguridad de la información, riesgos y continuidad del negocio y ciberseguridad, debidamente documentadas, implementadas, monitoreadas y auditables.
- 1.2. **EL CONTRATISTA** deberá contar con líneas base de seguridad o plantillas de hardening (proceso de fortalecer la seguridad de un sistema informático o red reduciendo su vulnerabilidad a ataques y otras amenazas) sobre los sistemas operativos, elementos de red, bases de datos, aplicaciones y cualquier dispositivo (desktop, laptop y/o equipos móviles, etc.) que sean utilizados de forma directa o indirecta para la prestación del servicio contratado por **CLARO COLOMBIA**. Estas guías de hardenización pueden estar construidas bajo estándares aceptados por la industria o lineamientos definidos por los fabricantes.
- 1.3. **EL CONTRATISTA** deberá contar con políticas, estándares y procedimientos definidos y auditables de control de acceso y manejo de perfiles sobre los sistemas o elementos de red que soporten el servicio contratado.
- 1.4. **EL CONTRATISTA** deberá contar con políticas, procedimientos y controles sobre los cambios que se realicen sobre cualquier infraestructura (software, hardware y middleware) que soporte el servicio contratado.
- 1.5. **EL CONTRATISTA** deberá contar con políticas de "escritorio limpio" para evitar la exposición de información confidencial.

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 4 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

- 1.6. **EL CONTRATISTA** declara conocer y se obliga a cumplir las normas **ISO 27001** y **PCI-DSS**. Que le apliquen de acuerdo con los procesos y servicios desarrollados para **CLARO COLOMBIA**.
- 1.7. **EL CONTRATISTA** deberá contar con cláusula de confidencialidad debidamente firmada con **CLARO COLOMBIA**.
- 1.8. **EL CONTRATISTA** se obliga a dar cumplimiento a los lineamientos establecidos por las **leyes 1266 de 2008 y 1581 de 2012**, así como sus decretos y circulares reglamentarios.
- 1.9. **EL CONTRATISTA** deberá contar con su propia política de tratamiento datos personales, alineado con los establecido en la **LEY 1581 DE 2012 – DECRETO 1377 DE 2013**.
- 1.10. **EL CONTRATISTA** deberá implementar mecanismos de anonimización o seudonimización, según corresponda, de acuerdo con el tipo de servicio prestado y la naturaleza de la información que custodie, especialmente cuando esta verse sobre datos personales sensibles; en cuyo caso **EL CONTRATISTA** se obliga a cumplir con los lineamientos aplicables al tratamiento de esta categoría de datos lo cual incluye pero no se limita a: informar previamente a los titulares el carácter facultativo del otorgamiento de autorización de tratamiento cuando estos versen sobre datos sensibles, implementar medidas de seguridad de la información adecuadas y suficientes para proteger los datos personales las cuales establecidas en este documento, y las instruidas por la Superintendencia de Industria y Comercio de Colombia, de conformidad con lo establecido en el Decreto 1377 de 2013 como demás normas que lo complementen adicionen o modifique, y en todo caso, no menores a las establecidas en la legislación vigente aplicable.
- 1.11. **EL CONTRATISTA** deberá exigir cláusula de confidencialidad a sus empleados y colaboradores, así como a sus terceros prestadores de servicio, los cuales interacción con servicios suministrados a **CLARO COLOMBIA**.
- 1.12. **EL CONTRATISTA** deberá exigir clausula contra el fraude y prevención de fuga de información a sus empleados y colaboradores.
- 1.13. **EL CONTRATISTA** deberá implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 5 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

- 1.14. **EL CONTRATISTA** deberá adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.
- 1.15. **EL CONTRATISTA** deberá realizar periódicamente campañas de concientización en seguridad de la información. Para prestación de servicios contratados como operaciones, agentes, centros de llamadas.
- 1.16. **EL CONTRATISTA** deberá establecer controles que impidan el ingreso a las áreas de actividades de dispositivos electrónicos (cámaras, celulares, USB, discos de almacenamiento externo, etc.) y elementos de escritura (cuadernos, lápices, hojas, etc.) o cualquier medio físico o electrónico que permita extraer información propiedad de **CLARO COLOMBIA**.
- 1.17. **EL CONTRATISTA** deberá establecer espacios para el almacenamiento de estos elementos personales, por fuera de las áreas de procesamiento de datos.
- 1.18. Es responsabilidad de **EL CONTRATISTA** validar los antecedentes del personal asignado a la prestación del servicio con **CLARO COLOMBIA**, deberá corroborar que no ha sido sancionado por problemas de confidencialidad de información o fallas profesionales, así mismo, ser consultado en SAGRILIFT.
- 1.19. **EL CONTRATISTA** deberá establecer cláusula en el contrato de los empleados que permita tomar acciones correctivas frente a la divulgación de información sensible posterior a la finalización del contrato.
- 1.20. **EL CONTRATISTA** deberá solicitar las autorizaciones de los Titulares para realizar la consulta de base de datos en centrales de riesgo, así como para la recolección, almacenamiento y tratamiento de datos personales.
- 1.21. **EL CONTRATISTA** deberá implementar los correspondientes controles que le permitan conservar y proteger la información que sea suministrada por **CLARO COLOMBIA** para la ejecución de los servicios contratados, impidiendo su deterioro, pérdida, alteración, uso no autorizado o fraudulento.

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 6 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

- 1.22. **EL CONTRATISTA** deberá atender los requerimientos que sean realizados por la Superintendencia de Industria y Comercio sobre los Titulares que hayan sido consultados.
- 1.23. **EL CONTRATISTA** deberá dar buen uso de los tokens u otros medios de doble autenticación, entregados para el acceso a los sistemas designados por **CLARO COLOMBIA**, cumpliendo con los controles necesarios para asegurar la confidencialidad de los datos que entregan estos dispositivos y dar cumplimiento a la cláusula de **CONTROL DE ACCESOS**, descrito en este documento.
- 1.24. **EL CONTRATISTA** deberá contar planes de continuidad que garanticen la prestación del servicio en todo momento, lo anterior incluye: infraestructura tecnológica, sistemas de información, canales de comunicación, recurso humano y su correspondiente escala de comunicaciones para manejo de eventos disruptivos. Así mismo **EL CONTRATISTA** deberá contar con las pruebas de verificación del plan de continuidad, con el fin de evidenciar que si se está ejecutando el plan.
- 1.25. **EL CONTRATISTA** deberá implementar los controles necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información de los clientes de **CLARO COLOMBIA**, cuando la misma sea transferida, procesada y/o almacenada en ambientes administrados por el mismo, adicionalmente deberá garantizar el borrado seguro de la información, cada vez que finalice el objetivo por el cual se entregó la información y posterior a la finalización de las relaciones contractuales entre las partes. Se debe entregar el certificado del borrado seguro ejecutado. – Gestores de borrado seguro. Revisar el proceso de reconstrucción
- 1.26. **EL CONTRATISTA** debe disponer de un proceso propio de gestión de vulnerabilidades técnicas, que le permita evaluar, identificar y tratar de forma oportuna las vulnerabilidades técnicas sobre las plataformas y sistemas de información que soporten servicios directos para **CLARO COLOMBIA** y/o para los clientes de este.
- 1.27. **EL CONTRATISTA** deberá proveer y mantener una cuenta de correo electrónico corporativo propia y debidamente gestionada, la cual será utilizada exclusivamente para fines relacionados con la prestación del servicio a **CLARO COLOMBIA**. Dicha cuenta deberá permitir la

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 7 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

recepción de códigos o notificaciones de validación asociados al doble factor de autenticación (MFA) requerido para el acceso seguro a los sistemas informáticos y plataformas que **CLARO COLOMBIA** le habilite.

- 1.28. **EI CONTRATISTA** deberá garantizar el uso seguro, responsable y conforme a las buenas prácticas de seguridad de la información de las cuentas de correo electrónico corporativo empleadas en la ejecución del servicio. Queda estrictamente prohibida cualquier actividad que pueda comprometer la confidencialidad, integridad o disponibilidad de la información, o que represente un riesgo para los activos, sistemas o datos de **CLARO COLOMBIA** a los cuales el **CONTRATISTA** tenga acceso.
- 1.29. **EI CONTRATISTA** estará obligado a garantizar la asignación de cuentas de correo corporativas al personal que se designe para la ejecución de los servicios en el marco del contrato suscrito con CLARO COLOMBIA, asegurando en todo momento la correcta segregación de permisos conforme al cargo y funciones asignadas, en cumplimiento de las políticas corporativas y normativas aplicables en materia de seguridad de la información.
- 1.30. **EI CONTRATISTA** será responsable de implementar controles que prevengan el uso indebido del correo, tales como autenticación multifactorial (MFA), protección antimalware, filtrado antiphishing y políticas de cifrado en el envío de información sensible.
- 1.31. **EL CONTRATISTA** deberá elaborar y mantener una matriz de riesgos de seguridad de la información y ciberseguridad, actualizada anualmente.
- 1.32. **EL CONTRATISTA** deberá contar con una metodología interna para la gestión de riesgos, la cual deberá contemplar la priorización de la remediación de estos, conforme a los criterios de criticidad definidos por **CLARO COLOMBIA**.
- 1.33. **EL CONTRATISTA** se obliga a Informar de manera inmediata a **CLARO COLOMBIA** y en ningún caso en un plazo no menor a un (1) día hábil desde el momento de ocurrencia del hecho o el momento en que en que el **CONTRATISTA** tenga conocimiento del hecho, de cualquier incidente de seguridad presentado que pueda comprometer la confidencialidad,

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 8 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

integridad o disponibilidad de los datos personales que el **CONTRATISTA** acceda o trate por instrucciones **CLARO COLOMBIA**.

- 1.34. **EL CONTRATISTA** se obliga a continuar con todas las investigaciones que resulten pertinentes tras la ocurrencia de cualquier hecho que afecte, o pueda afectar, la correcta ejecución de los servicios o el cumplimiento del objeto contractual celebrado con **CLARO COLOMBIA**. Asimismo, deberá entregar de manera oportuna y completa los informes, reportes y demás documentación que le sea requerida por **CLARO COLOMBIA** en relación con dicho acontecimiento.
- 1.35. **EL CONTRATISTA** se obliga a prestar apoyo a **COMCEL** en caso de requerimientos de autoridad competente relacionados con los datos personales a los que llegue acceder por instrucciones de **CLARO COLOMBIA** en calidad de encargado.

2. DESARROLLO DE SOFTWARE

- 2.1. **EL CONTRATISTA** debe contar con una metodología para cumplir el ciclo de desarrollo seguro de software la cual puede ser auditada por **CLARO COLOMBIA**, siempre y cuando el objeto del contrato sea el desarrollo de software y/o aplicaciones, para ello debe contemplar:

CICLO DE DESARROLLO SEGURO	
Requisitos	• Establecer requisitos de seguridad y privacidad. • Realizar evaluaciones de riesgos • de seguridad y privacidad.
Diseño	• Establecer requisitos de diseño. • Análisis / Reducción de vectores de ataque. • Modelamiento de amenazas.
Implementación	• Utilizar herramientas aprobadas. • Desactivar funciones inseguras. • Realizar análisis estático.
Verificación	• Realizar análisis de código estático. • Realizar análisis de composición de Software. • Realizar análisis dinámico. • Pruebas de Fuzzing (introducción deliberada de datos malformados o aleatorios). • Revisión de vectores de ataque.

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 9 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

Liberación	• Crear un plan de respuesta a incidentes. • Realizar la revisión final de seguridad. • Certificar software para puesta en producción.
Respuesta	• Ejecutar un plan de respuesta a incidentes y corrección de vulnerabilidades identificadas en el Sistema de información.

- 2.2. Dentro de los principios de diseño **EL CONTRATISTA** debe utilizar las últimas versiones estables de librerías de código abierto de fuentes reconocidas en la industria al momento de iniciar el desarrollo o modificación. No utilizar versiones beta, reuso (forks) ni de proyectos individuales o sin reconocer por la industria.
- 2.3. **EI CONTRATISTA** debe llevar el registro del control de cambios al desarrollo.
- 2.4. El código fuente en desarrollo debe ser protegido con el control de acceso adecuado, no se podrá acceder al mismo por parte de personal que no esté directamente involucrado en las tareas de desarrollo ni tampoco por terceras partes.
- 2.5. Para todo desarrollo que involucre transacciones, contenga información confidencial de los clientes o sus servicios, o constituyan un proceso de interacción de usuario final, **EL CONTRATISTA** deben capacitar por lo menos anualmente a sus desarrolladores, arquitectos, personal de pruebas, especialistas y demás personal que aplique, en las técnicas actualizadas de desarrollo seguro.
- 2.6. **EI CONTRATISTA** se compromete a contar con herramientas especializadas que permitan realizar pruebas de calidad del código y de seguridad del desarrollo con el objetivo de entregar un producto libre de malas prácticas de codificación y vulnerabilidades conocidas.
- 2.7. **EI CONTRATISTA** no podrá usar información de clientes de **CLARO COLOMBIA** para la ejecución.
- 2.8. **EL CONTRATISTA** no podrá tratar, utilizar, procesar, compartir, transmitir, transferir ni almacenar datos de clientes de **CLARO COLOMBIA** para fines distintos a los expresamente autorizados en el contrato suscrito entre las partes. Esto incluye, pero no se limita a, actividades de explotación comercial, desarrollo de plataformas o

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 10 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

soluciones para terceros, análisis con fines de negocio ajenos al objeto contractual, o cualquier otro uso que exceda el alcance definido o las instrucciones proporcionadas por **CLARO COLOMBIA**. Cualquier tratamiento de datos deberá realizarse conforme a la autorización de tratamiento de datos personales otorgada por los titulares, la política de tratamiento de datos personales aplicable, y previa valoración por parte de **CLARO COLOMBIA**.

- 2.9. El CONTRATISTA que incorpore, desarrolle, licencie o proporcione soluciones de inteligencia artificial (IA) que realicen el tratamiento de datos personales, deberá garantizar y cumplir sin excepciones los criterios y principios establecidos en la Leyes Estatutarias 1266 de 2008 y 1581 de 2012.
- 2.10. **EL CONTRATISTA** que incorpore, desarrolle, licencie o proporcione soluciones inteligencia artificial (IA), para la ejecución del servicio contratado para **CLARO COLOMBIA**, deberá establecer un programa que incorpore políticas, roles, responsabilidades, procesos de entrenamiento, protocolos de supervisión humana, criterios de decisión ante inconsistencias, procesos de evaluación de riesgo donde incluya exposición de datos personales incluidos sensibles, fallos en la validación y revisión periódica del ciclo de vida del sistema AI.
- 2.11. **EL CONTRATISTA** que incorpore, desarrolle, licencie o proporcione soluciones inteligencia artificial (IA), deberá ejecutar programa de pentesting, pruebas periódicas y seguimiento de mitigaciones identificadas.
- 2.12. **EL CONTRATISTA** que incorpore, desarrolle, licencie o proporcione soluciones inteligencia artificial (IA), deberá establecer un programa de simulación y defensa contra la manipulación de datos de entrenamiento, controles en el proceso de ingestión de datos, con el fin de proteger los modelos de IA frente a alteraciones maliciosas que puedan comprometer su comportamiento.
- 2.13. **EL CONTRATISTA** que incorpore, desarrolle, licencie o proporcione soluciones inteligencia artificial (IA), deberá implementar un proceso de revisión de las APIs utilizadas por sistemas de IA, que incluya autenticación robusta.

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 11 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

- 2.14. **EI CONTRATISTA** que incorpore, desarrolle, licencie o proporcione soluciones basadas en inteligencia artificial (IA) estará obligado a garantizar que dichas soluciones, tanto en ambientes de desarrollo como en ambientes de producción, correspondan a soluciones corporativas que cumplan con los criterios y estándares de seguridad exigidos para la adecuada prestación del servicio objeto del presente contrato.
- 2.15. **EL CONTRATISTA** que incorpore, desarrolle, licencie o proporcione soluciones o servicios basados en inteligencia artificial (IA), se obliga a garantizar, implementar, realizar o documentar un estudio de impacto de privacidad (*privacy impact assesment*), cuando quiera que se identifique que el diseño, desarrollo o implementación de una solución de inteligencia artificial (IA) pueda comportar un riesgo de afectación de información de los titulares, el cual deberá contener:
- (a) Una descripción detallada de las operaciones de tratamiento de datos personales.
 - (b) Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales. en la evaluación de riesgos se espera, por lo menos, la identificación y clasificación estos.
 - (c) Las medidas previstas para evitar la materialización de los riesgos, medidas de seguridad, diseño de software, tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los titulares de los datos y de otras personas que pueda eventualmente resultar afectadas.
- 2.16. **EL CONTRATISTA** que incorpore, desarrolle, licencie o proporcione soluciones de datos o servicios basados en inteligencia artificial (IA), deberá garantizar que la solución haya sido elaborada bajo métodos que contemplen la privacidad por diseño y por defecto (*privacy by design*), lo cual implica el uso de métodos técnicos, matemáticos, de programación que contemplen entre otros; la realización de analítica de datos sin revelar la información de los titulares que proporcionaron los datos, la anonimización de información, la recolección de la información estrictamente necesaria para las finalidades del tratamiento, entre otra.

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 12 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

2.17. **EL CONTRATISTA** que incorpore desarrolle, licencie o proporcione soluciones o servicios basados en inteligencia artificial (IA), cumplir con las medidas de seguridad adecuadas según se establecen en este documento, la legislación aplicable, y aquellas instruidas por la Superintendencia de Industria y Comercio, lo cual implica la adopción de medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole para evitar:

- (a) El acceso indebido o no autorizado a los datos personales.
- (b) La manipulación de la información.
- (c) La destrucción de la información.
- (d) El uso indebido o no autorizado de la información a personas no autorizadas.

Las medidas de seguridad implementadas deben ser auditables por **CLARO COLOMBIA** y las autoridades competentes, para su evaluación y mejora permanente.

3. CONECTIVIDAD EXTERNA CON LA RED DE CLARO

3.1. **EL CONTRATISTA** debe contar con conexiones cifradas para garantizar la confidencialidad e integridad de la información que es intercambiada con **CLARO COLOMBIA**.

3.2. **EL CONTRATISTA** deberá cumplir con las siguientes condiciones técnicas:

- a) **Interfaces físicas:** Compatibilidad en los tipos de interfaz y verificación de las conexiones.
- b) **Última milla:** Disponibilidad controlada.
- c) **Ubicación y espacio:** Reservar la ubicación y el espacio de los elementos, garantizar el control de temperatura / condiciones ambientales (humedad, temperatura, disipación térmica, ruido, ventilación, etc.)
- d) **Control de acceso:** Procedimientos implementados de control de acceso físico y lógico sobre los equipos que soportan el servicio.
- e) **Aislamiento de manera lógica:** Aislar virtualmente el tráfico con los otros segmentos de red conectados en el mismo dispositivo o dominio.

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 13 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

- f) **Servicios de NAT (Network Address Traslation):** Deberán ser conciliados entre las partes para el correcto funcionamiento de las aplicaciones y la correcta asignación de direcciones IP.
- g) **Servicios de PAT (Port Address Traslation):** Los servicios PAT están restringidos y no deben ser configurados.
- h) **Documentación del servicio:** Ingeniera de detalle de la red que soportara los servicios. Seguridad perimetral: Contar con Firewall y mecanismos de conexión cifrada de extremo a extremo.
- 3.3. **EL CONTRATISTA** deberá asegurar de extremo a extremo los canales de comunicación y garantizar que los mismos no sean susceptibles de ser manipulados o conocidos por personal ajeno a la prestación del servicio.
- 3.4. **EL CONTRATISTA** deberá implementar herramientas de cifrado de disco, VPN corporativa y MFA, y gestión de dispositivos móviles (MDM) para todo personal en modalidad remota.
- 3.5. **EL CONTRATISTA** deberá realizar revisiones semestrales para verificar el cumplimiento de las políticas de seguridad de la información por parte de los colaboradores que se encuentren en modalidad de teletrabajo.
- 3.6. Los dispositivos de red de **EL CONTRATISTA** que se involucren en la conectividad deberán estar convenientemente protegidos y asegurados.
- 3.7. **EL CONTRATISTA** deberá contar con controles perimetrales que garanticen la confidencialidad, disponibilidad e integridad de la información de **CLARO COLOMBIA**.
- 3.8. **EL CONTRATISTA** no hará uso de protocolos o servicios de comunicación inseguros (no cifrados) y deberá deshabilitar, de cualquier dispositivo de red, aquellos servicios que no sean necesarios o utilizados.
- 3.9. **EL CONTRATISTA** deberá monitorear continuamente sus sistemas y redes para detectar actividades sospechosas o intentos de intrusión.
- 3.10. Todos los servidores o estaciones involucradas con actividades del servicio prestado a **CLARO COLOMBIA** que se ubiquen en la red de **EL CONTRATISTA** deberán estar convenientemente aislados en una zona independiente. Estos servidores no deberán ubicarse lógicamente en zonas expuestas a tráfico proveniente de internet (por ejemplo, la zona

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 14 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

DMZ) ni tampoco convivir con servidores de **EL CONTRATISTA** que no estén relacionados con la operación del servicio prestado a **CLARO COLOMBIA**.

- 3.11. **EL CONTRATISTA** deberá contar con estándares de direccionamiento para redes privadas.
- 3.12. **EL CONTRATISTA** deberá realizar análisis periódicos, al menos una vez al año, respecto a vulnerabilidades técnicas sobre los dispositivos de red involucrados en la prestación del servicio, así mismo, deberá dar cierre oportuno a cualquier brecha de seguridad identificada por medio de esta actividad. **CLARO COLOMBIA** en cualquier momento, podrá desarrollar dichos ejercicios, previa coordinación y validación con **EL CONTRATISTA**.
- 3.13. **EL CONTRATISTA** deberá contar con mecanismos que permitan realizar la trazabilidad punta a punta de cualquier evento de operación o seguridad que se genere durante la prestación del servicio.

4. EQUIPOS DE CONTRATISTA EN EJECUCIÓN DEL CONTRATO.

EL CONTRATISTA se obliga a que todos los equipos de trabajo que utilice en la ejecución del contrato:

- 4.1. Contarán con sistemas de antivirus, antispyware y/o antimalware licenciados, legalmente adquiridos y vigentes.
- 4.2. Contarán con sistemas operativos, bases de datos y herramientas de ofimática soportadas por el fabricante.
- 4.3. Contarán con su propio dominio de correo electrónico; está prohibido el uso de correo de dominio público.
- 4.4. Contarán con procedimientos claramente definidos y de ejecución periódica para implementación de actualizaciones de seguridad (parches) en las plataformas.
- 4.5. Contarán con repositorios lógicos y/o físicos de información internos y con controles de acceso claramente definidos para garantizar que no será expuesta información confidencial de **CLARO COLOMBIA**.

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 15 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

- 4.6. Los equipos de funcionalidad portable deberán está debidamente cifrado, así mismo, el contratista deberá contar con un repositorio de credenciales.
- 4.7. Los usuarios asignados por el contratista deberán estar basado en el menor privilegio requerido para el correcto desempeño de sus funciones.
- 4.8. **EL CONTRATISTA** deberá prohibir la conexión o instalación no autorizada de cualquier clase de dispositivo de comunicaciones o software que modifique o revise la topología de la red de la organización.
- 4.9. **EL CONTRATISTA** deberá establecer políticas y procedimientos adecuados y debidamente autorizados por la gerencia de seguridad de la información de **CLARO COLOMBIA** para realizar copias de seguridad de la información, la misma deberá estar cifrada.
- 4.10. **EI CONTRATISTA** deberá garantizar un borrado seguro de la información propiedad de **CLARO COLOMBIA** en los siguientes casos: A) Finalice el contrato, B) el usuario responsable sea retirado de proyecto con **CLARO COLOMBIA** o es retirado de la compañía, C) Renovación de tecnología o tecnología obsoleta, D) Información histórica no requerida por el proyecto. Así mismo, deberá dar notificación oportuna a **CLARO COLOMBIA** solicitando la debida autorización.
- 4.11. **EL CONTRATISTA** deberá realizar mantenimiento preventivo a los equipos que asegure su disponibilidad y su integridad.
- 4.12. El software utilizado por **EL CONTRATISTA** para prestar el servicio a **CLARO COLOMBIA** debe ser usado dentro de los términos y condiciones establecidos en su licenciamiento, lo cual incluye las restricciones de uso establecidas en las licencias de software libre. Lo anterior aplica indiferentemente si el software se instala en algún equipo de **EL CONTRATISTA** o es accedido por el mismo en la plataforma de un tercero en modalidad software como servicio. Cualquier condición de licenciamiento que brinde al fabricante o representante del software o de la plataforma, a cambio del uso de la herramienta, algún tipo de derecho sobre la información que **CLARO COLOMBIA** comparte con el proveedor de inmediato hace no viable el uso de dicho software
- 4.13. **EI CONTRATISTA** será responsable frente a los incidentes que se puedan generar por la instalación incontrolada de Software, cuya

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 16 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

consecuencia sea fuga, perdidas de integridad y/ o genere indisponibilidad de la información propiedad de **CLARO COLOMBIA**, así como por la violación de los derechos de propiedad intelectual en la que lleguen a incurrir.

- 4.14. **EI CONTRATISTA** deberá implementar guías de configuración y/o hardenización en cada uno de los componentes de tecnología que estarán conectados a la red de **CLARO COLOMBIA**.
- 4.15. **EI CONTRATISTA** se compromete a no enviar información considerada sensible o confidencial a través de plataformas de mensajería instantánea (incluye WhatsApp, Telegram, Messenger, etc).

5. EQUIPOS DE CONTRATISTA EN LA RED DE CLARO

EL CONTRATISTA se obliga a que todos los equipos de trabajo que utilice en la ejecución del contrato estarán sujetos al cumplimiento de los siguientes lineamientos y estándares.

- 5.1. Cumplir con las políticas, procedimientos y estándares de seguridad de **CLARO COLOMBIA**.
- 5.2. Estar registrados en el dominio o dominios de **CLARO COLOMBIA**.
- 5.3. Contar con un usuario y contraseña el cual es personal e intransferible.
- 5.4. Contar con sistemas de antivirus, antispyware y/o antimalware debidamente licenciados y legalmente adquiridos. Si **CLARO COLOMBIA** lo considera conveniente se podrá instalar el antivirus corporativo en las estaciones de **EL CONTRATISTA** durante la ejecución del contrato.
- 5.5. **EI CONTRATISTA** deberá informar oportunamente a **CLARO COLOMBIA** cuando un colaborador suyo haya dejado de prestar sus servicios.
- 5.6. Ningún colaborador del **EL CONTRATISTA** deberá retirar información de **CLARO COLOMBIA** de sus instalaciones sin la autorización previa y escrita de un representante de CLARO.

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 17 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

- 5.7. Los equipos deberán tener única y exclusivamente el software autorizado por **CLARO COLOMBIA**.
- 5.8. Antes de finalizar el contrato, **EL CONTRATISTA** debe garantizar o permitir un borrado seguro de la información propiedad de **CLARO COLOMBIA**.
- 5.9. **EL CONTRATISTA** entiende y acepta que no está permitido el uso de medios removibles o unidades de almacenamiento externas que no sean proporcionados por **CLARO COLOMBIA**.
- 5.10. Permitir la instalación de software proveído por **CLARO COLOMBIA**.

6. CONTROL DE CAMBIOS Y AUDITORIAS DE SEGURIDAD

- 6.1. **EL CONTRATISTA** estará en la obligación de comunicar oportunamente a **CLARO COLOMBIA** cualquier cambio a la infraestructura (software, hardware y middleware) que soporte el servicio contratado y pueda afectar directa o indirectamente el nivel de seguridad establecido. De igual manera **EL CONTRATISTA** estará sujeto a revisiones periódicas y/o auditorías por parte de **CLARO COLOMBIA**, de acuerdo con la solicitud expresa por el área de Seguridad de la Información, las cuales serán acordadas con el ánimo de verificar el cumplimiento de los requerimientos de seguridad y realizar las observaciones y recomendaciones del caso.
- 6.2. **EL CONTRATISTA** deberá estar dispuesto en cuanto a la atención y respuesta de las auditorías realizadas por Seguridad de la Información.
- 6.3. **EL CONTRATISTA** deberá someterse a visitas anuales, o en cualquier momento en que **CLARO COLOMBIA** lo requiera, conforme al cronograma acordado entre las partes o cuando se evidencien anomalías en la ejecución del servicio.
- 6.4. **EL CONTRATISTA** deberá entregar las evidencias correspondientes a las visitas realizadas por la Gerencia de Seguridad de la Información, ya sea como parte de su planificación o bajo solicitud puntual. Estas evidencias deberán estar relacionadas con el cumplimiento de

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 18 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

actividades tales como escaneo de vulnerabilidades, campañas de concientización, reportes de auditoría interna, ejecución de controles técnicos de seguridad, entre otras.

- 6.5. **EL CONTRATISTA** deberá mantener registros actualizados sobre el cumplimiento y la remediación de hallazgos durante toda la vigencia del contrato, asegurando su conservación en el tiempo.

7. CONTROL DE ACCESO

- 7.1. Al recibir un usuario y una contraseña, **EL CONTRATISTA** acepta las condiciones establecidas por **CLARO COLOMBIA** y se compromete a dar el uso adecuado y a mantener el carácter de confidencialidad que ella otorga. En ninguna circunstancia, **EL CONTRATISTA** está autorizado a compartir sus usuarios y claves. Es responsabilidad de **EL CONTRATISTA** transmitir a las personas a su cargo el carácter confidencial, privado e intransferible de los usuarios y contraseñas que **CLARO COLOMBIA** otorga a cada uno. En el mismo sentido se considerará un incumplimiento grave el hecho de compartir cualquier tipo de usuario o contraseña. De detectarse y comprobarse esta conducta, **CLARO COLOMBIA**, tomará todas las acciones disciplinarias, penalizaciones o sanciones definidas contractualmente a las que haya lugar.
- 7.2. Participar activamente en el proceso de certificación y depuración de cuentas de usuarios, confirmando la existencia de sus usuarios y reportando irregularidades detectadas.
- 7.3. Ser el responsable por el buen uso de los accesos otorgados a plataformas de **CLARO COLOMBIA**.
- 7.4. Informar de manera inmediata a **CLARO COLOMBIA** cualquier incidente de seguridad presentado con los accesos otorgados por CLARO.
- 7.5. Informar de manera inmediata a **CLARO COLOMBIA**, las bajas o cambios con relación a privilegios de acceso debido a retiros, transferencias y/o cambios de funciones o actividades.

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 19 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

- 7.6. Cada vez que se aprovisiona una cuenta de usuario en los sistemas de información de **CLARO COLOMBIA** se debe asegurar la veracidad e integridad de la información ingresada en los requerimientos para identificar de manera inequívoca el responsable del acceso.
- 7.7. Los accesos a sistemas que tenga autorizado **EL CONTRATISTA** y que por operación se deba tener implementado el múltiple factor de autenticación, **EL CONTRATISTA** estará en la obligación de realizar las configuraciones correspondientes para su implementación.
- 7.8. **EI CONTRATISTA** debe asegurarse de que sus factores de autenticación estén protegidos de manera adecuada para evitar su interceptación o uso indebido.
- 7.9. Las cuentas de usuario que sean definidas por **EL CONTRATISTA** deben ser únicas y deben estar constituidas bajo un dominio corporativo (NO GMAIL, HOTMAIL, YAHOO, etc.), esto con el fin de evitar que se materialicen riesgos de seguridad de la información.
- 7.10. **EL CONTRATISTA** deberá garantizar que el personal asignado para la prestación de servicios a **CLARO COLOMBIA** no sea destinado simultáneamente a otros servicios, proyectos o unidades de negocio del mismo **CONTRATISTA**, ni de terceros.
- 7.11. **EI CONTRATISTA** deberá implementar controles internos que aseguren la dedicación exclusiva del personal asignado, así como mecanismos de trazabilidad y supervisión que permitan verificar el cumplimiento de esta disposición.

8. PLAZO DE IMPLEMENTACION DE OBLIGACIONES POR PARTE DEL CONTRATISTA

- 8.1. **EL CONTRATISTA** contará con un plazo máximo de 2 meses contados a partir de la firma del contrato u otro si para dar cumplimiento a los lineamientos establecidos en el presente Anexo.
- 8.2. **EL CONTRATISTA** dispondrá de un plazo máximo de 60 días calendario después de ser notificado, para corregir las vulnerabilidades identificadas durante el escaneo y/o Ethical Hacking solicitados por

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 20 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

CLARO COLOMBIA. Premisas: Cualquier actualización a este anexo o las políticas de **CLARO COLOMBIA**, serán de estricto cumplimiento para **EL CONTRATISTA**.

9. ALMACENAMIENTO Y MANEJO DE INFORMACIÓN EN NUBE

- 9.1. **EI CONTRATISTA** deberá utilizar únicamente las nubes privadas autorizadas por **CLARO COLOMBIA** (Oracle OCI, Microsoft Azure, Amazon AWS y Google Cloud), asegurando la prioridad de los recursos definidos por la organización.
- 9.2. **EI CONTRATISTA** deberá asegurar la disposición final de la información almacenada, procesada y/o transmitida en cada una de las nubes autorizadas por **CLARO COLOMBIA** de acuerdo con las buenas prácticas de seguridad (ISO 27001, PCI DSS, SOX, etc.) y estándares de la industria (NIST, ISO, CIS, etc.), dando cumplimiento con las políticas de seguridad dispuestas por la organización.
- 9.3. **EI CONTRATISTA** deberá cumplir con lo dispuesto en el numeral 3.2 de la circular externa 008 de 2017 de la Superintendencia de Industria y Comercio (SIC): "Países que cuentan con un nivel adecuado de protección de datos personales". En caso contrario que el proyecto o iniciativa NO cumpla con lo dispuesto por la SIC, no se dará la aprobación por parte de la Gerencia de Seguridad de la Información.
- 9.4. **EI CONTRATISTA** deberá cumplir con lo definido en el convenio de Budapest acerca de los delitos cibernéticos y los países que hacen parte de este convenio.
- 9.5. **EI CONTRATISTA** deberá disponer de backups (copias de seguridad) de la información en distintos puntos geográficos como protección contra interrupciones y pérdidas.

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 21 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

10. INCUMPLIMIENTOS

El proceso de cobro de los incumplimientos se realizará de acuerdo con el procedimiento liquidar incumplimientos de aliados y proveedores y las actualizaciones que se realicen posteriormente y divulgadas por Claro

10.1. **Tabla de incumplimientos:** Para efectos de los requerimientos de seguridad e la información, riesgos y continuidad de terceros se impondrán las multas con base en la siguiente tabla:

ITEM	CAPITULO DEL ANEXO TECNICO DE SEGURIDAD	DESCRIPCIÓN	FRECUENCIA	# SMLDV del año en curso
1	Cumplimiento normativo o regulatorio	Se refiere a la obligación que tienen los aliados de adherirse a las leyes y regulaciones aplicables a su sector, esto incluye aspectos como la protección de datos, seguridad de la información, protección de datos de tarjetahabiente, etc. La multa es aplicable cuando EI CONTRATISTA incumpla con las normativas de protección de datos personales, estándares internacionales como ISO 27001 y PCI DSS.	Cada vez que se presente	30
2	Desarrollo de software	Se refiere al proceso de crear y mantener aplicaciones o sistemas informáticos, que incluye desde la planificación hasta la implementación siguiendo metodologías de codificación segura. La multa es aplicable cuando EL CONTRATISTA que en sus efectos realice procesos de desarrollo seguro, incumpla con la implementación de una metodología de codificación segura o NO presente pruebas de seguridad como Pentesting o análisis de vulnerabilidades.	Cada vez que se presente	30

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 22 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

3	Conectividad externa con la red de Claro	Se refiere a la capacidad de una organización para vincularse y comunicarse de manera segura con redes externas como proveedores, aliados o plataformas, permitiendo el intercambio de datos e información. Se aplicará la multa correspondiente cuando EI CONTRATISTA incumpla con las condiciones técnicas establecidas dentro del Anexo.	Cada vez que se presente	15
4	Equipos contratista en ejecución del contrato	Se refieren a los grupos de trabajo o personal que un aliado asigna para llevar a cabo las actividades y tareas específicas en un contrato. Se aplicará la multa correspondiente cuando EL CONTRATISTA incumpla con cualquiera de las condiciones de del numeral 4 de este Anexo.	Cada vez que se presente	15
5	Equipos de contratista en la red de Claro	Son los grupos de trabajo asignados por un aliado para realizar tareas relacionadas con la instalación, mantenimiento o actualización de la red de CLARO COLOMBIA . Se aplicará la multa correspondiente cuando EL CONTRATISTA incumpla con cualquiera de las condiciones descritas dentro del punto 5 de este anexo.	Cada vez que se presente	15
6	Control de cambios y auditorías de seguridad	Gestiona y autoriza modificaciones en sistemas para evitar riesgos de seguridad, mientras que las auditorías de seguridad revisan regularmente las políticas y las prácticas de seguridad implementadas en la organización. Se aplicará la multa correspondiente cuando EL CONTRATISTA incumpla con las revisiones periódicas de seguridad y no se evidencien los cierres de los hallazgos correspondientes.	Cada vez que se presente	15

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 23 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

7	Control de acceso	Implementación de políticas y sistemas implementados para restringir el acceso a datos, aplicaciones o recursos dentro de una red. Se aplicará la multa correspondiente cuando EL CONTRATISTA incumpla con los lineamientos definidos para el acceso seguro a las aplicaciones, sistemas de información o datos.	Cada vez que se presente	30
8	Plazo de implementación	Periodo de tiempo determinado para llevar a cabo la ejecución de un plan de acción de acuerdo con los hallazgos encontrados en un proceso de auditoría. Se aplicará la multa correspondiente cuando EL CONTRATISTA incumpla con los tiempos de remediación de los planes de acción y/o cierre de vulnerabilidades críticas y altas que puedan significar la materialización de un riesgo para Claro Colombia.	Cada vez que se presente	20
9	Almacenamiento y manejo de información en nube	Se refiere a la implementación, configuración y administración de los servicios que se tienen contratados en la nube, pudiendo acceder a los archivos y aplicaciones desde cualquier lugar y en cualquier momento. Se aplicará la multa correspondiente cuando EL CONTRATISTA incumpla con cualquiera de las condiciones de del numeral 9 de este Anexo.	Cada vez que se presente	30

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 24 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.

ANEXO 5 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	Fecha: 28/01/2026	
Clasificación: Uso Interno	Versión: 01	

11.CONTROL DE VERSIONES

Versión	Cambio realizado	Responsable del cambio	Fecha cambio
0	Versión inicial.	Gerencia Seguridad Informática	2011
1	Se amplía el alcance del capítulo #2 Desarrollo de Software, Se adicionan los ítems 2.2, 2.3, 2.4, 2.5, 2.6, 2.7	Gerencia Seguridad Información	2021
2	Se adicionan los ítems 1.4, 3.6, 4.14, 4.15	Gerencia Seguridad Información	2023
3	Se adiciona las condiciones que debe cumplir el contratista para servicios de Nube	Gerencia de Seguridad	2024
4	Se efectuaron cambios estructurales en la siguiente sección, correspondientes al ajuste y/o modificación de las directrices allí establecidas: 1.Cumplimiento Normativo y Regulatorio (Tratamiento de Datos Personales) 2. Desarrollo de Software 3. Conectividad Externa con la red de Claro 4. Equipos de contratistas en la ejecución del Contrato 6. Controles de Cambios y Auditorías de Seguridad	Gerencia Seguridad de la Información	2026

Clasificación: Uso Interno	RESPONSABLE	Cargo del responsable	APROBÓ	Cargo del responsable
	APOYO MEJORA CONTINUA			Pág. 25 de 25

Se prohíbe la reproducción parcial o total de este documento, así como su impresión o digitalización sin permiso previo de la Gerencia Mejora Continua de Procesos Corporativos, favor consultar en el portal del Sistema Integral de Gestión la versión vigente. Cualquier copia del documento se considera copia no controlada.