ANEXO N°4

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

GERENCIA DE SEGURIDAD DE LA INFORMACION

Tabla de Contenido

RESPONSABLE	**Gerencia de Seguridad de la Información**

ANEXO 4 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	**Fecha:**05-06-2024	
CLASIFICACIÓN: USO INTERNO	VERSIÓN: 09	

OBJETIVO

RESPONSABLE	**Gerencia de Seguridad de la Información**

Establecer los requerimientos mínimos de seguridad 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 de COMCEL S.A., y/o INFRACEL S.A. E.S.P (en adelante CLARO) y Operadora de pagos móviles S.A.S.

ALCANCE:

Todo tercero, proveedor, distribuidor, aliado y/o contratista de CLARO, 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. Dado que EL CONTRATISTA es el único y directo responsable de la operación y aseguramiento de toda su infraestructura, deberá ser consciente y convenientemente actualizado de los riesgos y amenazas de seguridad que puedan surgir; en este sentido deberá contar con políticas y procedimientos complementarios a los lineamientos y estándares aquí establecidos, que le aseguren el establecimiento y mantenimiento niveles óptimos de seguridad.

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

1. CUMPLIMIENTO NORMATIVO O REGULATORIO.

RESPONSABLE	**Gerencia de Seguridad de la Información**

1.1 EL CONTRATISTA deberá contar con políticas, procedimientos, estándares y/o metodologías de seguridad de la información, riesgos y continuidad del negocio, debidamente documentadas, implementadas, monitoreadas y auditables.

1.2 EL CONTRATISTA deberá contar con líneas base de seguridad o plantillas de hardening sobre los sistemas operativos, elementos de red, bases de datos, aplicaciones y cualquier dispositivo (desktop, laptop y/o equipos móviles) que sea utilizados para la prestación del servicio contratado por CLARO. 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.

1.4 EL CONTRATISTA deberá contar con políticas de "escritorio limpio" para evitar la exposición de información confidencial.

1.5 EL CONTRATISTA declara conocer y se obliga a cumplir las normas ISO27001 y PCI-DSS. Que le apliquen de acuerdo con los procesos y servicios desarrollados para Claro.

1.6 EL CONTRATISTA deberá contar con cláusula de confidencialidad debidamente firmada con CLARO.

1.7 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.

1.8 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.

1.9 EL CONTRATISTA deberá exigir cláusula de confidencialidad a sus empleados y colaboradores.

1.10 EL CONTRATISTA deberá exigir clausula contra el fraude y prevención de fuga de información a sus empleados y colaboradores.

1.11 EL CONTRATISTA deberá implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.

1.12 EL CONTRATISTA deberá adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles. EL CONTRATISTA deberá realizar periódicamente campañas de concientización en seguridad de la información. Para prestación de servicios contratados como operaciones, agentes, centros de llamadas, 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.

EL CONTRATISTA deberá establecer espacios para el almacenamiento de estos elementos.

1.13 Es responsabilidad de EL CONTRATISTA validar los antecedentes del personal asignado a la prestación del servicio con CLARO, deberá corroborar que no ha sido sancionado por problemas de confidencialidad de información o fallas profesionales, así mismo, ser consultado en SAGRILAFT.

1.14 EL CONTRATISTA deberá establecer cláusula en el contrato del empleado que permita tomar acciones correctivas frente a la divulgación de información sensible posterior a la finalización del contrato.

1.15 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.

1.16 EL CONTRATISTA deberá implementar los correspondientes controles que le permitan conservar y proteger la información que sea suministrada por Claro para la ejecución de los servicios contratados, impidiendo su deterioro, pérdida, alteración, uso no autorizado o fraudulento.

1.17 EL CONTRATISTA deberá atender los requerimientos que sean realizados por la Superintendencia de Industria y Comercio sobre los Titulares que hayan sido consultados.

1.18 EL CONTRATISTA deberá dar buen uso de los tokens entregados para el acceso a los sistemas designados por CLARO, 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 ACCESO, descrito en este documento.

1.19 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.

1.20 EL CONTRATISTA deberá implementar los controles necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información de los clientes de Claro, 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.

1.21 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 y/o para los clientes del mismo.

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, siempre y cuando el

objeto del contrato sea el desarrollo de software y/o aplicaciones, para ello debe contemplar:

- Entrenamiento de seguridad

- 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

• 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, reúso (forks) ni de proyectos individuales o sin reconocer por la industria.

2.3 El 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 este 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. El 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.

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.

3.2 EL CONTRATISTA deberá cumplir con las siguientes condiciones técnicas:

Interfaces físicas: Compatibilidad en los tipos de interfaz y verificación de las conexiones.

Última milla: Disponibilidad controlada.

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.)

Control de acceso: Procedimientos implementados de control de acceso físico y lógico sobre los equipos que soportan el servicio.

Aislamiento de manera lógica: Aislar virtualmente el tráfico con los otros segmentos de red conectados en el mismo dispositivo o dominio.

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.

Servicios de PAT (Port Address Traslation): Los servicios PAT están restringidos y no deben ser configurados.

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 Los dispositivos de red de EL CONTRATISTA que se involucren en la conectividad deberán estar convenientemente protegidos y asegurados.

3.5 EL CONTRATISTA deberá contar con controles perimetrales que garanticen la confidencialidad, disponibilidad e integridad de la información de CLARO.

3.6 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.

3.6 EL CONTRATISTA deberá monitorear continuamente sus sistemas y redes para detectar actividades sospechosas o intentos de intrusión.

3.7 Todos los servidores o estaciones involucradas con actividades del servicio prestado a CLARO 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 DMZ) ni tampoco convivir con servidores de EL CONTRATISTA que no estén relacionados con la operación del servicio prestado a CLARO.

3.8 EL CONTRATISTA deberá contar con estándares de direccionamiento para redes privadas.

3.9 EL CONTRATISTA deberá realizar análisis periódicos de 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 en cualquier momento, podrá desarrollar dichos ejercicios, previa coordinación y validación con EL CONTRATISTA.

3.10 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.

4.6 Los equipos de funcionabilidad 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 para realizar copias de seguridad de la información, la misma deberá estar cifrada.

4.10 El CONTRATISTA deberá garantizar un borrado seguro de la información propiedad de CLARO en los siguientes casos: A) Finalice el contrato, B) el usuario responsable sea retirado de proyecto con CLARO 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 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 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 del 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 comparte con el proveedor de inmediato hace no viable el uso de dicho software.

4.13 El CONTRATISTA será responsable frente a los incidentes que se puedan generar por la instalación incontrolada de Software, cuya consecuencia sea fuga, perdidas de integridad y/ o genere indisponibilidad de la información propiedad de Claro, así como por la violación de los derechos de propiedad intelectual en la que lleguen a incurrir.

4.14 El 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 El 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.

5.2 Estar registrados en el dominio o dominios de CLARO.

5.3 Contar con un usuario y password el cual es personal e intransferible.

5.4 Contar con sistemas de antivirus, antispyware y/o antimalware debidamente licenciados y legalmente adquiridos. Si CLARO lo considera conveniente se podrá instalar el antivirus corporativo en las estaciones de EL CONTRATISTA durante la ejecución del contrato.

5.5 El CONTRATISTA deberá informar oportunamente a CLARO cuando un colaborador suyo haya dejado de prestar sus servicios.

5.6 Ningún colaborador del CONTRATISTA deberá retirar información de CLARO de sus instalaciones sin la autorización previa y escrita de un representante de CLARO.

5.7 Los equipos deberán tener única y exclusivamente el software autorizado por CLARO.

5.8 Antes de finalizar el contrato, el CONTRATISTA debe garantizar o permitir un borrado seguro de la información propiedad de CLARO.

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.

5.10 Permitir la instalación de software proveído por CLARO.

6. CONTROL DE CAMBIOS Y AUDITORIAS DE SEGURIDAD

6.1 EL CONTRATISTA estará en la obligación de comunicar oportunamente a CLARO 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 auditorías por parte de CLARO, que 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.

7. CONTROL DE ACCESO

7.1 Al recibir un usuario y una contraseña, EL CONTRATISTA acepta las condiciones establecidas por CLARO 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 del CONTRATISTA transmitir a las personas a su cargo el carácter confidencial, privado e intransferible de los usuarios y contraseñas que CLARO 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, 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.

7.4 Informar de manera inmediata a CLARO cualquier incidente de seguridad presentado con los accesos otorgados por CLARO.

7.5 Informar de manera inmediata a CLARO, las bajas o cambios con relación a privilegios de acceso debido a retiros, trasferencias y/o cambios de funciones o actividades.

7.6 Cada vez que se aprovisione una cuenta de usuario en los sistemas de información de CLARO se debe asegurar la veracidad e integridad de la información ingresada en los requerimientos para identificar de manera inequívoca el responsable del acceso.

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

9. ALMACENAMIENTO Y MANEJO DE INFORMACIÓN EN NUBE

9.1 El 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 El 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 El 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 El 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 El CONTRATISTA deberá disponer de Backups de la información en distintos puntos geográficos como protección contra interrupciones y perdidas.

10. INCUMPLIMIENTO

Cuando al CONTRATISTA incumpla cualquiera de las obligaciones establecidas en el anexo, CLARO podrá imponer multas equivalentes al uno por ciento (1%) del valor del Contrato por cada día de retraso en el cumplimiento de sus obligaciones.

RESPONSABLE	**Gerencia de Seguridad de la Información**

CONTROL DE VERSIONES

Versión	Cambio realizado	Responsable del cambio	Fecha cambio
0	Versión inicial.	Gerencia Seguridad Informática	2011
1	Se adicionan ITEM de cumplimiento para seguridad Informática	Gerencia Seguridad Informática	2012
2	Se adicionan ITEM de cumplimiento para seguridad Informática	Gerencia de Seguridad Informática	2015
3	Se Ajustan y adicionan cumplimientos normativos o regulatorios, conectividad externa con la red de claro, equipos de contratista en la red de claro y en ejecución de contrato, control de cambios y auditorias. Y se incluye numeral 8 sobre incumplimiento	Gerencia Seguridad Información	2017

RESPONSABLE	Gerencia de Seguridad de la Información

4	Eliminación de Telmex en el objetivo del documento. Se amplía el alcance del presente anexo a órdenes de compra. Numeral 1. Se aclara que toda política o procedimiento debe estar debidamente documentado y debe ser auditable. Se aclara cuando aplica el cumplimiento de la ISO 27001 PCI DSS. Se ajusta ítem con relación a la administración de los tokens. Numeral 2. Se incluye capítulo de desarrollo de software. Numeral 3. Se ajusta la introducción Se ajusta punto relacionado con Planes de contingencia. Numeral 4. Sé elimina el ítem relacionado con usó de equipos personales, lo cual no está autorizado.	Gerencia Seguridad Información	2020
Versión	**Cambio realizado**	**Responsable del cambio**	**Fecha cambio**
	Se incluye ítem relacionado con el software instalado y utilizado en los pc´s. Numeral 5. Se ajusta ítem relacionado con los sistemas de antivirus y antispyware. Numeral 7. Se corrige Comcel por Claro. Numeral 8. Se incluye tiempo máximo para corregir vulnerabilidades. Numeral 9. Se ajusta redacción.		

RESPONSABLE	**Gerencia de Seguridad de la Información**

	Numeral 10. Se organiza el ítem de control de cambios de la versión		
5	Se ajusta número de versión Se adiciona al ítem de cumplimiento normativo y regulatorio el numeral 1.28 Relacionado con los planes de continuidad, el cual no debería estar en el ítem de conectividad.	Gerencia Seguridad Información	2020
6	Se ajusta número de versión Se adiciona el ítem 1.8 , 1.30 y 1.31 relacionado a análisis de vulnerabilidades, protección de la información, borrado seguro y ley	Gerencia Seguridad Información	2020
7	Se amplia el alcance del capitulo #2 Desarrollo de Software, Se adicionan los ítems 2.2, 2.3, 2.4, 2.5, 2.6, 2.7	Gerencia Seguridad Información	2021
8	Se adicionan los ítems 1.4 , 3.6 , 4.14 , 4.15	Gerencia Seguridad Información	2023
9	Se adiciona las condiciones que debe cumplir el contratista para servicios de Nube	Gerencia de Seguridad	2024

RESPONSABLE	**Gerencia de Seguridad de la Información**

RESPONSABLE	**Gerencia de Seguridad de la Información**

ANEXO 4 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACION, RIESGOS Y CONTINUIDAD DE TERCEROS		
CONTRATISTA Y SUBCONTRATISTA DE CLARO	**Fecha:**02-08-2023	
CLASIFICACIÓN: USO INTERNO	VERSIÓN: 08	

RESPONSABLE	**Gerencia de Seguridad de la Información**