CONDICIONES Y RESTRICCIONES RESPONSABILIDADES DEL CLIENTE Y CLARO

Servicios CSOC Esencial – CSOC PLATINUM Estratégico

4.1 Naturaleza Jurídica del Servicio SOC

Qué es:

El servicio CSOC de Claro Colombia, en todos sus niveles, se entiende jurídicamente como una obligación de medio y no de resultado. Esto significa que Claro se compromete a prestar el servicio con diligencia profesional, usando herramientas adecuadas, personal especializado y buenas prácticas, pero no puede garantizar que nunca sucederá un incidente de ciberseguridad.

Por qué es así:
Porque en ciberseguridad:

- No existe tecnología infalible.
- No se controla todo el entorno (usuarios, decisiones, procesos internos del cliente, terceros, etc.).
- El atacante tiene iniciativa, recursos y capacidad de evolucionar.

Por lo tanto, sería jurídicamente inviable asumir una obligación de resultado (garantizar que no haya incidentes), ya que excede el control real y razonable de Claro.

Hasta dónde va:
Claro se obliga a:

- Monitorear, analizar y correlacionar eventos.
- Notificar incidentes detectados dentro del alcance.
- Acompañar técnicamente según el nivel de servicio contratado.

Pero no se obliga a eliminar el riesgo ni a evitar cualquier incidente, ni a asegurar que no se materialicen daños.

4.1.1 Condiciones de Alcance Operativo y Prestación del Servicio CSOC

Para la correcta prestación del servicio CSOC de Claro Colombia, es necesario que se cumplan determinadas **condiciones operativas, técnicas y de información**, las cuales delimitan el alcance efectivo del servicio y garantizan una operación adecuada, consistente y alineada con el modelo de responsabilidad compartida.

El servicio CSOC se presta sobre la base de la **información y fuentes de eventos que sean formalmente integradas**, para lo cual **el cliente deberá proporcionar y mantener actualizado**, como mínimo:

- El **inventario de activos** a ser monitoreados (direcciones IP, rangos, equipos, servidores, aplicaciones, entornos y tecnologías incluidas).
- La identificación de las **plataformas de seguridad, infraestructura y sistemas** que generarán eventos y telemetría (EDR/XDR, dispositivos de red, sistemas, aplicaciones, entre otros).
- Los **accesos técnicos, conectividad y configuraciones necesarias** para la correcta ingesta de eventos en la plataforma CSOC, conforme a los lineamientos definidos durante la etapa de implementación.

El alcance del servicio CSOC se limita exclusivamente a los **activos, tecnologías y fuentes de información declaradas e integradas**, no siendo responsable Claro Colombia por eventos, incidentes o amenazas que se originen en activos no informados, no integrados o fuera del alcance acordado.

Condiciones de Licenciamiento y Componentes Tecnológicos

El servicio CSOC corresponde a un **servicio gestionado de monitoreo, análisis, correlación y acompañamiento en ciberseguridad**, y **no incluye el licenciamiento de las plataformas, herramientas o tecnologías de seguridad del cliente**, salvo que se indique expresamente lo contrario en la propuesta comercial.

El licenciamiento de soluciones tales como **EDR, XDR, firewalls, plataformas de seguridad, herramientas de análisis u otras tecnologías**, cuando aplique, será contratado de manera independiente al servicio CSOC, ya sea directamente por el cliente o a través de acuerdos comerciales específicos con Claro Colombia.

Condiciones de Alcance Económico y Responsabilidades Pecuniarias

El servicio CSOC **no constituye un seguro, póliza de cobertura financiera ni garantía económica** frente a incidentes de ciberseguridad. En consecuencia, Claro Colombia **no asume responsabilidad pecuniaria** por:

- Pérdidas económicas directas o indirectas derivadas de incidentes de seguridad.
- Interrupciones del negocio, lucro cesante o afectación de ingresos.
- Daños reputacionales, sanciones regulatorias o costos legales.

- Fraudes, extorsiones, ransomware, pagos a terceros o recuperación financiera posterior a un incidente.

La responsabilidad de Claro Colombia se limita a la **prestación diligente del servicio conforme al alcance contratado**, bajo el principio de obligación de medio, y en ningún caso implicará la asunción del riesgo financiero, operativo o legal inherente a la operación del negocio del cliente.

4.2 Alcance y Limitación de la Responsabilidad de Claro Colombia

La responsabilidad de Claro Colombia en la prestación del servicio CSOC se encuentra estrictamente delimitada por el **alcance del servicio contratado**, las **condiciones operativas acordadas** y el principio de **obligación de medio** definido en el presente documento.

Claro Colombia es responsable de prestar el servicio CSOC con la debida diligencia profesional, utilizando personal especializado, herramientas tecnológicas adecuadas y buenas prácticas de la industria, conforme al nivel de servicio contratado. Sin embargo, dicha responsabilidad **no implica la asunción del riesgo inherente a la operación del negocio**, ni la garantía de que no ocurran incidentes de ciberseguridad.

En consecuencia, Claro Colombia **no asume responsabilidad** por eventos, incidentes o impactos que se originen en:

- Activos, sistemas, infraestructuras o tecnologías que no hayan sido declarados, inventariados o integrados formalmente al alcance del servicio.
- Decisiones operativas, técnicas o estratégicas adoptadas por el cliente, incluyendo la no aplicación de recomendaciones, parches o acciones de mitigación sugeridas.
- Configuraciones inseguras, falta de mantenimiento, obsolescencia tecnológica o debilidades preexistentes en el entorno tecnológico del cliente.
- Acciones u omisiones de usuarios, empleados, proveedores, terceros o aliados del cliente.

Desde el punto de vista económico, el servicio CSOC **no constituye una póliza de seguro, garantía financiera ni cobertura de pérdidas**, por lo que Claro Colombia no asume responsabilidad pecuniaria por pérdidas económicas, interrupciones del negocio, lucro cesante, sanciones regulatorias, daños reputacionales, fraudes,

extorsiones, ransomware o cualquier otro impacto financiero derivado de un incidente de seguridad.

El presente marco de responsabilidad se complementa con el **modelo de responsabilidad compartida** descrito en la sección 4.3, bajo el cual cada parte asume responsabilidades de acuerdo con su rol, control y capacidad de decisión.

4.3 Modelo de Responsabilidad Compartida

La prestación del servicio CSOC de Claro Colombia se rige por un **modelo de responsabilidad compartida**, en el cual cada parte asume responsabilidades de acuerdo con su **rol, nivel de control y capacidad de decisión** sobre el entorno tecnológico y el negocio.

- Este modelo reconoce que, si bien Claro Colombia provee capacidades especializadas de monitoreo, análisis, correlación y acompañamiento en ciberseguridad, **la gestión integral del riesgo, la operación del negocio y la toma de decisiones estratégicas permanecen bajo responsabilidad del cliente**.

Responsabilidades de Claro Colombia

En el marco del servicio CSOC y conforme al nivel de servicio contratado, Claro Colombia es responsable de:

- Operar el CSOC bajo un esquema de **monitoreo continuo 7x24x365**, utilizando personal especializado, procesos definidos y herramientas adecuadas.
- Recolectar, ingerir, normalizar y correlacionar eventos de seguridad provenientes de las fuentes de información formalmente integradas al alcance del servicio.
- Aplicar reglas de detección, analítica avanzada, inteligencia de amenazas y, cuando aplique, automatización y orquestación para la identificación de eventos e incidentes de seguridad.
- Clasificar, priorizar y notificar incidentes de seguridad conforme a los SLAs definidos para cada modelo de servicio.
- Acompañar técnicamente la respuesta a incidentes, proporcionando análisis, recomendaciones y orientación especializada, sin asumir la ejecución directa de acciones operativas salvo acuerdo expreso.

- Mantener la confidencialidad de la información tratada y cumplir con la normativa aplicable en materia de protección de datos y seguridad de la información.

Responsabilidades del Cliente

El cliente, como propietario de los activos, la información y los procesos de negocio, es responsable de:

- Definir y mantener actualizado el **inventario de activos, tecnologías y fuentes de información** incluidas en el servicio CSOC.
- Proveer los **accesos técnicos, conectividad, configuraciones y autorizaciones necesarias** para la correcta integración y operación del servicio.
- Administrar, operar y mantener su infraestructura tecnológica, plataformas de seguridad y sistemas de información.
- Evaluar y ejecutar las recomendaciones técnicas entregadas por el CSOC, incluyendo acciones de mitigación, contención, corrección o mejora.
- Tomar las **decisiones operativas, técnicas y estratégicas** relacionadas con la continuidad del negocio, priorización de sistemas, aplicación de parches y gestión del riesgo.
- Cumplir con las obligaciones legales, regulatorias y contractuales aplicables a su sector y operación.

Alcance del Modelo de Responsabilidad Compartida

El modelo de responsabilidad compartida implica que:

- Claro Colombia **no asume la administración integral de la infraestructura**, ni sustituye las funciones internas de TI, Seguridad, Riesgo o Gobierno del cliente.

Capacidad operativa nacional

Tiene presencia real en Colombia, cobertura geográfica, equipos especializados y conocimiento del entorno local, regulatorio y empresarial. Esto permite actuar con criterio y rapidez, conociendo las necesidades específicas de las organizaciones

colombianas y las particularidades de su ecosistema tecnológico y normativo.
Esto se traduce en:

- Soporte con contexto local.
- Respuestas y procedimientos adaptados a las realidades regulatorias (por ejemplo, cumplimiento de la Ley 1581 y normativa sectorial).
- Operación estable en todo el territorio colombiano.

Soporte garantizado cuando más importa

Cuando ocurre un incidente, lo que realmente importa no es la tecnología… sino **el aliado que responde**.
Con Claro usted obtiene:

- **Expertos disponibles**, preparados para apoyar en momentos críticos.
- **Acompañamiento real**, basado en metodologías estructuradas.
- **Soporte operativo y técnico**, no solo reportes.

No es simplemente "un proveedor tecnológico" es **un socio de operación**.

Procesos maduros y probados

Claro no aprende sobre la marcha, opera con metodologías consolidadas, gobierno de seguridad estructurado y disciplina operativa, lo que garantiza:

- Acciones trazables y documentadas
- Gestión estandarizada y repetible
- Calidad verificable en cada intervención

Cada operación del CSOC se basa en procesos profesionales que optimizan la detección, análisis y respuesta ante amenazas, lo cual se traduce en **resultados medibles y consistentes**.

ANEXO A – CONDICIONES OPERATIVAS POR NIVEL DE SERVICIO CSOC

Estas condiciones definen la naturaleza jurídica y operativa de la oferta comercial.

- **Naturaleza del Servicio (Obligación de Medio):** Jurídicamente, el servicio se define como una obligación de medio y no de resultado. Claro se compromete a monitorear y gestionar con diligencia profesional, pero **no garantiza la**

inexistencia de incidentes, dado que la tecnología no es infalible y el entorno no está 100% controlado.

- **Alcance Operativo:** El servicio se limita exclusivamente a los activos (IPs, servidores, aplicaciones) que hayan sido **formalmente inventariados e integrados** en la plataforma. Claro no responde por eventos en activos no declarados.
- **Responsabilidad Económica:** El servicio **no es un seguro** ni una póliza financiera. Claro no asume responsabilidad pecuniaria por lucro cesante, extorsiones (Ransomware), fraudes bancarios o daños reputacionales derivados de un ciberataque.

Capacidad operativa nacional

Tiene presencia real en Colombia, cobertura geográfica, equipos especializados y conocimiento del entorno local, regulatorio y empresarial. Esto permite actuar con criterio y rapidez, conociendo las necesidades específicas de las organizaciones colombianas y las particularidades de su ecosistema tecnológico y normativo.
Esto se traduce en:

- Soporte con contexto local.
- Respuestas y procedimientos adaptados a las realidades regulatorias (por ejemplo, cumplimiento de la Ley 1581 y normativa sectorial).
- Operación estable en todo el territorio colombiano.

Soporte garantizado cuando más importa

Cuando ocurre un incidente, lo que realmente importa no es la tecnología… sino **el aliado que responde**.
Con Claro usted obtiene:

- **Expertos disponibles**, preparados para apoyar en momentos críticos.
- **Acompañamiento real**, basado en metodologías estructuradas.
- **Soporte operativo y técnico**, no solo reportes.

No es simplemente “un proveedor tecnológico” es **un socio de operación**.

Procesos maduros y probados

Claro no aprende sobre la marcha, opera con metodologías consolidadas, gobierno de seguridad estructurado y disciplina operativa, lo que garantiza:

- Acciones trazables y documentadas
- Gestión estandarizada y repetible
- Calidad verificable en cada intervención

Cada operación del CSOC se basa en procesos profesionales que optimizan la detección, análisis y respuesta ante amenazas, lo cual se traduce en **resultados medibles y consistentes**.

ANEXO A – CONDICIONES OPERATIVAS POR NIVEL DE SERVICIO CSOC

Estas condiciones definen la naturaleza jurídica y operativa de la oferta comercial.

- **Naturaleza del Servicio (Obligación de Medio):** Jurídicamente, el servicio se define como una obligación de medio y no de resultado. Claro se compromete a monitorear y gestionar con diligencia profesional, pero **no garantiza la inexistencia de incidentes**, dado que la tecnología no es infalible y el entorno no está 100% controlado.
- **Alcance Operativo:** El servicio se limita exclusivamente a los activos (IPs, servidores, aplicaciones) que hayan sido **formalmente inventariados e integrados** en la plataforma. Claro no responde por eventos en activos no declarados.
- **Responsabilidad Económica:** El servicio **no es un seguro** ni una póliza financiera. Claro no asume responsabilidad pecuniaria por lucro cesante, extorsiones (Ransomware), fraudes bancarios o daños reputacionales derivados de un ciberataque.
- **Licenciamiento:** El servicio no incluye las licencias de las herramientas del cliente (Firewalls, EDR, XDR), salvo que se especifique en la oferta comercial. El cliente debe tener su licenciamiento vigente.
- **Responsabilidad Compartida:** Claro aporta la capacidad de monitoreo y análisis, pero la **toma de decisiones estratégicas** (ej. apagar un servicio crítico, aplicar un parche riesgoso) y la gestión del riesgo del negocio permanecen bajo la responsabilidad del cliente.

1. RESTRICCIONES ESPECÍFICAS POR MODELO

1.1. CSOC ESENCIAL – ALCANCE DEL SERVICIO

Qué incluye el CSOC Esencial

El CSOC Esencial incluye monitoreo proactivo e ininterrumpido 24/7/365 sobre los activos declarados, permitiendo la detección y correlación de eventos de seguridad en tiempo real. El servicio consolida la información proveniente de las fuentes integradas y genera alertas validadas, clasificadas y contextualizadas según su nivel de criticidad.

Incluye la gestión de alertas, orientada a notificar oportunamente a la organización sobre eventos relevantes que puedan afectar la confidencialidad, integridad o disponibilidad de los sistemas. También incorpora reportes de amenazas globales, que permiten conocer tendencias y campañas activas a nivel mundial.

El servicio contempla canales formales de atención a través de plataforma ITSM, mesa de servicio especializada y atención telefónica, garantizando trazabilidad en la gestión de requerimientos.

Incluye reportería operacional con informe técnico mensual, reporte de eventos, resumen ejecutivo, sesiones de seguimiento y dashboards de visualización que presentan el estado de los activos y alertas alineadas al marco MITRE ATT&CK.

Qué no incluye el CSOC Esencial

El CSOC Esencial no incluye actividades de búsqueda proactiva de amenazas (Threat Hunting), ni análisis de correos sospechosos, ni ejecución de archivos en sandbox. No contempla respuesta a incidentes, contención, erradicación ni recuperación. Tampoco incluye escaneo de vulnerabilidades, inteligencia de amenazas dedicada (CTI), mesa de crisis, informes de incidentes ni reportes de vulnerabilidades.

Este modelo no ejecuta acciones correctivas ni intervenciones sobre la infraestructura del cliente. Su alcance se limita a la detección, análisis y notificación.

1.2. CSOC PLATINUM – ALCANCE DEL SERVICIO

Qué incluye el CSOC PLATINUM

El CSOC PLATINUM incluye todo lo contemplado en el modelo Esencial, e incorpora capacidades de defensa integral para la gestión de incidentes críticos.

Incluye respuesta a incidentes mediante una bolsa de horas anual, que cubre análisis, contención, apoyo en erradicación y acompañamiento en recuperación, bajo

activación formal del cliente. Incorpora escaneo de vulnerabilidades para identificar debilidades en sistemas, servidores o aplicaciones, previa autorización.

Incluye Cyber Threat Intelligence (CTI) dedicada, con inteligencia contextualizada al sector, tipo de negocio y perfil de riesgo de la organización, permitiendo anticipar campañas dirigidas y actores relevantes.

Este modelo entrega reportes avanzados, incluyendo reporte de vulnerabilidades, informe detallado de incidentes y reportes de inteligencia.

Qué no incluye el CSOC PLATINUM

El CSOC PLATINUM no reemplaza funciones legales, forenses ni de aseguradoras. No asume la notificación a autoridades en nombre del cliente. No garantiza la erradicación total de amenazas ni la inexistencia de incidentes. No incluye servicios de representación legal, peritaje judicial ni gestión de pólizas de seguro.

Tiene presencia real en Colombia, cobertura geográfica, equipos especializados y conocimiento del entorno local, regulatorio y empresarial. Esto permite actuar con criterio y rapidez, conociendo las necesidades específicas de las organizaciones colombianas y las particularidades de su ecosistema tecnológico y normativo.
Esto se traduce en:

- Soporte con contexto local.
- Respuestas y procedimientos adaptados a las realidades regulatorias (por ejemplo, cumplimiento de la Ley 1581 y normativa sectorial).
- Operación estable en todo el territorio colombiano.

Soporte garantizado cuando más importa

Cuando ocurre un incidente, lo que realmente importa no es la tecnología… sino **el aliado que responde**.
Con Claro usted obtiene:

- **Expertos disponibles**, preparados para apoyar en momentos críticos.
- **Acompañamiento real**, basado en metodologías estructuradas.
- **Soporte operativo y técnico**, no solo reportes.

No es simplemente “un proveedor tecnológico” es **un socio de operación**.

Procesos maduros y probados

Claro no aprende sobre la marcha, opera con metodologías consolidadas, gobierno de seguridad estructurado y disciplina operativa, lo que garantiza:

- Acciones trazables y documentadas
- Gestión estandarizada y repetible
- Calidad verificable en cada intervención

Cada operación del CSOC se basa en procesos profesionales que optimizan la detección, análisis y respuesta ante amenazas, lo cual se traduce en **resultados medibles y consistentes**.

ANEXO A – CONDICIONES OPERATIVAS POR NIVEL DE SERVICIO CSOC

Estas condiciones definen la naturaleza jurídica y operativa de la oferta comercial.

- **Naturaleza del Servicio (Obligación de Medio):** Jurídicamente, el servicio se define como una obligación de medio y no de resultado. Claro se compromete a monitorear y gestionar con diligencia profesional, pero **no garantiza la inexistencia de incidentes**, dado que la tecnología no es infalible y el entorno no está 100% controlado.
- **Alcance Operativo:** El servicio se limita exclusivamente a los activos (IPs, servidores, aplicaciones) que hayan sido **formalmente inventariados e integrados** en la plataforma. Claro no responde por eventos en activos no declarados.
- **Responsabilidad Económica:** El servicio **no es un seguro** ni una póliza financiera. Claro no asume responsabilidad pecuniaria por lucro cesante, extorsiones (Ransomware), fraudes bancarios o daños reputacionales derivados de un ciberataque.
- **Licenciamiento:** El servicio no incluye las licencias de las herramientas del cliente (Firewalls, EDR, XDR), salvo que se especifique en la oferta comercial. El cliente debe tener su licenciamiento vigente.
- **Responsabilidad Compartida:** Claro aporta la capacidad de monitoreo y análisis, pero la **toma de decisiones estratégicas** (ej. apagar un servicio crítico, aplicar un parche riesgoso) y la gestión del riesgo del negocio permanecen bajo la responsabilidad del cliente.

1. RESTRICCIONES ESPECÍFICAS POR MODELO

1.1. CSOC ESENCIAL – ALCANCE DEL SERVICIO

Qué incluye el CSOC Esencial

El CSOC Esencial incluye monitoreo proactivo e ininterrumpido 24/7/365 sobre los activos declarados, permitiendo la detección y correlación de eventos de seguridad en tiempo real. El servicio consolida la información proveniente de las fuentes integradas y genera alertas validadas, clasificadas y contextualizadas según su nivel de criticidad.

Incluye la gestión de alertas, orientada a notificar oportunamente a la organización sobre eventos relevantes que puedan afectar la confidencialidad, integridad o disponibilidad de los sistemas. También incorpora reportes de amenazas globales, que permiten conocer tendencias y campañas activas a nivel mundial.

El servicio contempla canales formales de atención a través de plataforma ITSM, mesa de servicio especializada y atención telefónica, garantizando trazabilidad en la gestión de requerimientos.

Incluye reportería operacional con informe técnico mensual, reporte de eventos, resumen ejecutivo, sesiones de seguimiento y dashboards de visualización que presentan el estado de los activos y alertas alineadas al marco MITRE ATT&CK.

Qué no incluye el CSOC Esencial

El CSOC Esencial no incluye actividades de búsqueda proactiva de amenazas (Threat Hunting), ni análisis de correos sospechosos, ni ejecución de archivos en sandbox. No contempla respuesta a incidentes, contención, erradicación ni recuperación. Tampoco incluye escaneo de vulnerabilidades, inteligencia de amenazas dedicada (CTI), mesa de crisis, informes de incidentes ni reportes de vulnerabilidades.

Este modelo no ejecuta acciones correctivas ni intervenciones sobre la infraestructura del cliente. Su alcance se limita a la detección, análisis y notificación.

1.2. CSOC PLATINUM – ALCANCE DEL SERVICIO

Qué incluye el CSOC PLATINUM

El CSOC PLATINUM incluye todo lo contemplado en el modelo Esencial, e incorpora capacidades de defensa integral para la gestión de incidentes críticos.

Incluye respuesta a incidentes mediante una bolsa de horas anual, que cubre análisis, contención, apoyo en erradicación y acompañamiento en recuperación, bajo activación formal del cliente. Incorpora escaneo de vulnerabilidades para identificar debilidades en sistemas, servidores o aplicaciones, previa autorización.

Incluye Cyber Threat Intelligence (CTI) dedicada, con inteligencia contextualizada al sector, tipo de negocio y perfil de riesgo de la organización, permitiendo anticipar campañas dirigidas y actores relevantes.

Este modelo entrega reportes avanzados, incluyendo reporte de vulnerabilidades, informe detallado de incidentes y reportes de inteligencia.

Qué no incluye el CSOC PLATINUM

El CSOC PLATINUM no reemplaza funciones legales, forenses ni de aseguradoras. No asume la notificación a autoridades en nombre del cliente. No garantiza la erradicación total de amenazas ni la inexistencia de incidentes. No incluye servicios de representación legal, peritaje judicial ni gestión de pólizas de seguro.