

CISO as a Service

Protección Integral para la Seguridad de la Información de su Empresa

¿Qué es CISO as a Service?

En el entorno empresarial colombiano actual, la seguridad de la información se ha convertido en un pilar fundamental para la continuidad y competitividad de las organizaciones. El servicio de CISO as a Service (Chief Information Security Officer como Servicio) de **Sisteseg** ofrece a las empresas colombianas acceso a un ejecutivo de seguridad de alto nivel sin la necesidad de contratar a tiempo completo a un profesional interno, optimizando costos mientras se mantiene el más alto estándar de protección de activos digitales.

Un CISO tradicional representa una inversión significativa para cualquier organización: salarios competitivos, beneficios, capacitación continua y recursos de soporte. Para muchas empresas pequeñas y medianas en Colombia, esta inversión puede resultar prohibitiva, dejándolas vulnerables ante un panorama de amenazas cada vez más sofisticado. Nuestro modelo de CISO as a Service democratiza el acceso a expertise de clase mundial en seguridad de la información, permitiendo que organizaciones de todos los tamaños cuenten con liderazgo estratégico en ciberseguridad.

El Panorama de Amenazas en Colombia

Colombia enfrenta desafíos únicos en materia de ciberseguridad. El país ha experimentado un incremento sostenido en ciberataques dirigidos a organizaciones de todos los sectores: financiero, salud, manufactura, retail y servicios. Los ataques de ransomware, el phishing dirigido, la filtración de datos y el fraude digital representan riesgos reales que pueden paralizar operaciones, generar pérdidas millonarias y dañar irreparablemente la reputación corporativa.

La transformación digital acelerada, impulsada por la pandemia y las nuevas dinámicas de trabajo remoto e híbrido, ha ampliado la superficie de ataque de las organizaciones. Cada dispositivo conectado, cada aplicación en la nube, cada colaborador trabajando desde casa representa un punto de entrada potencial para los ciberdelincuentes. En este contexto, contar con un CISO experimentado no es un lujo, sino una necesidad estratégica.

¿Qué Incluye Nuestro Servicio de CISO?

El servicio de CISO as a Service de Sisteseg va mucho más allá de una simple consultoría. Nos convertimos en parte integral de su equipo ejecutivo, asumiendo la responsabilidad completa de diseñar, implementar y gestionar su programa de seguridad de la información. Nuestros servicios incluyen:

Gobernanza y Estrategia de Seguridad

Desarrollamos e implementamos un marco de gobernanza de seguridad adaptado a su organización, alineado con estándares internacionales como ISO 27001, NIST, y regulaciones colombianas vigentes. Esto incluye la definición de políticas, procedimientos y estándares de seguridad que establecen las bases para una cultura de seguridad robusta en toda la organización.

Nuestro CISO trabaja directamente con su junta directiva y equipo ejecutivo para definir el apetito de riesgo organizacional, establecer objetivos de seguridad alineados con la estrategia de negocio, y asegurar que las inversiones en seguridad generen valor tangible. Desarrollamos roadmaps estratégicos plurianuales que evolucionan con su negocio y el panorama de amenazas.

Gestión de Riesgos y Cumplimiento

Realizamos evaluaciones exhaustivas de riesgos de seguridad de la información, identificando vulnerabilidades críticas, amenazas relevantes y el impacto potencial en sus operaciones. Desarrollamos e implementamos planes de tratamiento de riesgos que priorizan acciones según su impacto en el negocio y viabilidad de implementación.

Mantenemos a su organización en cumplimiento con regulaciones colombianas como la Ley de Protección de Datos Personales (Ley 1581 de 2012), las circulares de la Superintendencia Financiera para entidades del sector, y estándares internacionales relevantes para su industria. Preparamos a su organización para auditorías y certificaciones, coordinando todos los esfuerzos necesarios para lograr y mantener el cumplimiento.

Diseño e Implementación de Arquitectura de Seguridad

Diseñamos arquitecturas de seguridad robustas que protegen sus activos críticos sin comprometer la productividad. Esto incluye la definición de controles técnicos, administrativos y físicos apropiados para su contexto organizacional. Evaluamos, seleccionamos e implementamos tecnologías de seguridad como firewalls de nueva generación, sistemas de detección y prevención de intrusiones, soluciones de protección de endpoints, gestión de identidades y accesos, y plataformas de análisis de seguridad.

Trabajamos con su equipo de TI para integrar la seguridad en cada etapa del ciclo de vida de desarrollo de sistemas, promoviendo prácticas de DevSecOps que incorporan seguridad desde el diseño. Aseguramos que las migraciones a la nube, las implementaciones de nuevas tecnologías y las transformaciones digitales se realicen con seguridad como prioridad fundamental.

Gestión de Incidentes y Respuesta a Crisis

Desarrollamos e implementamos capacidades de respuesta a incidentes que permiten a su organización detectar, contener y recuperarse rápidamente de eventos de seguridad. Esto incluye la creación de un equipo de respuesta a incidentes (CSIRT), procedimientos de escalamiento, playbooks de respuesta para diferentes tipos de incidentes, y la coordinación con autoridades y stakeholders externos cuando sea necesario.

Realizamos simulacros regulares de ciberataques (tabletop exercises) para validar y mejorar continuamente sus capacidades de respuesta. En caso de un incidente real, nuestro CISO asume el liderazgo de la respuesta, coordinando esfuerzos técnicos, comunicaciones con stakeholders, decisiones de negocio y restauración de operaciones.

Gestión de Terceros y Cadena de Suministro

Evaluamos y gestionamos los riesgos de seguridad introducidos por proveedores, socios y terceros que tienen acceso a sus sistemas o datos. Desarrollamos procesos de due diligence de seguridad

para nuevos proveedores, establecemos requisitos contractuales de seguridad, y monitoreamos continuamente el desempeño de seguridad de su ecosistema de terceros.

La seguridad de la cadena de suministro se ha convertido en un vector de ataque cada vez más explotado. Nuestro enfoque integral asegura que los eslabones débiles en su cadena de valor no se conviertan en puertas de entrada para atacantes sofisticados.

Concientización y Capacitación en Seguridad

El factor humano sigue siendo el eslabón más débil en la mayoría de las organizaciones. Desarrollamos e implementamos programas comprensivos de concientización en seguridad que transforman a sus colaboradores de vulnerabilidades potenciales en la primera línea de defensa contra amenazas cibernéticas.

Nuestros programas incluyen capacitaciones presenciales y virtuales, campañas de phishing simulado, materiales de comunicación atractivos y medibles, y evaluaciones periódicas de efectividad. Adaptamos los contenidos a diferentes roles y niveles de riesgo dentro de la organización, asegurando relevancia y engagement máximo.

Ventajas del Modelo CISO as a Service

Acceso a Expertise de Clase Mundial

Nuestros CISOs cuentan con certificaciones internacionales de prestigio como CISSP, CISM, CRISC, y años de experiencia liderando programas de seguridad en organizaciones de diversos sectores. Al contratar nuestro servicio, obtiene acceso inmediato a este conocimiento especializado sin los meses de reclutamiento y onboarding que requeriría un CISO interno.

Además, nuestro modelo permite que usted se beneficie del conocimiento acumulado de nuestro equipo completo. Cuando su CISO asignado enfrenta un desafío particular, puede recurrir a la experiencia colectiva de Sisteseq, incluyendo especialistas en diferentes dominios de seguridad, analistas de amenazas, y expertos técnicos.

Costo-Efectividad Comprobada

El costo de contratar un CISO de tiempo completo en Colombia puede oscilar entre \$120 y \$200 millones de pesos anuales, sin considerar beneficios, bonificaciones y costos de infraestructura de soporte. Nuestro servicio de CISO as a Service representa una fracción de esta inversión, típicamente entre 40% y 60% del costo de un CISO interno, mientras proporciona cobertura más amplia y acceso a recursos adicionales.

Esta optimización de costos no implica sacrificar calidad o dedicación. Nuestro modelo está diseñado para proporcionar la atención y el tiempo necesarios para cada cliente, con compromisos claros de disponibilidad y tiempos de respuesta garantizados.

Flexibilidad y Escalabilidad

Las necesidades de seguridad de su organización no son estáticas. Pueden incrementarse durante proyectos de transformación digital, adquisiciones, lanzamiento de nuevos productos o en

respuesta a incidentes de seguridad. Nuestro modelo permite escalar el nivel de servicio según sus necesidades cambiantes, sin los compromisos rígidos de una posición de tiempo completo.

Puede comenzar con un engagement de pocas horas mensuales para evaluación y planificación, y escalar hacia un modelo más robusto a medida que desarrolla su programa de seguridad. Esta flexibilidad es especialmente valiosa para organizaciones en crecimiento o aquellas navegando cambios significativos.

Perspectiva Externa e Independiente

Un CISO interno puede enfrentar presiones políticas organizacionales, conflictos de interés, o resistencia al cambio por parte de stakeholders establecidos. Nuestro CISO externo aporta una perspectiva independiente y objetiva, basada en mejores prácticas de la industria y experiencia con múltiples organizaciones.

Esta independencia es particularmente valiosa al presentar evaluaciones de riesgo honestas a la junta directiva, al recomendar inversiones significativas en seguridad, o al implementar cambios de proceso que pueden encontrar resistencia interna. Nuestro CISO actúa como su advocate de seguridad, sin agendas ocultas ni compromisos políticos internos.

Continuidad Garantizada

La rotación de personal es un riesgo real. Si su CISO interno renuncia o toma licencia extendida, su programa de seguridad puede quedar a la deriva durante meses mientras recluta y capacita a un reemplazo. Con nuestro servicio, la continuidad está garantizada. Si su CISO asignado no está disponible, otro miembro de nuestro equipo con contexto completo de su organización asume inmediatamente, sin interrupciones en la protección de sus activos.

Nuestro Proceso de Implementación

Fase 1: Evaluación y Planificación (Mes 1-2)

Iniciamos cada engagement con una evaluación comprensiva del estado actual de su seguridad de la información. Esto incluye entrevistas con stakeholders clave, revisión de documentación existente, evaluación de controles técnicos implementados, y análisis de incidentes de seguridad previos.

El resultado de esta fase es un informe ejecutivo que documenta hallazgos críticos, gaps frente a mejores prácticas y estándares relevantes, y un roadmap priorizado de iniciativas de seguridad. Este roadmap se convierte en el norte estratégico para los siguientes 12-24 meses, con hitos claros, responsables asignados y métricas de éxito definidas.

Fase 2: Quick Wins y Remediación Crítica (Mes 2-4)

Basándonos en la evaluación inicial, identificamos e implementamos "quick wins" - mejoras de alto impacto que pueden realizarse rápidamente con recursos limitados. Esto genera momentum, demuestra valor tangible a stakeholders, y reduce riesgos críticos en el corto plazo.

Simultáneamente, priorizamos la remediación de vulnerabilidades críticas identificadas. Esto puede incluir la implementación de autenticación multifactor, el endurecimiento de

configuraciones de sistemas críticos, la segmentación de redes, o el despliegue de soluciones de protección de endpoints donde no existan.

Fase 3: Construcción de Fundamentos (Mes 4-9)

Con los riesgos inmediatos bajo control, nos enfocamos en construir los fundamentos de un programa de seguridad maduro y sostenible. Esto incluye el desarrollo e implementación de políticas y procedimientos formales, la estructuración de un proceso de gestión de riesgos continuo, el establecimiento de métricas e indicadores de desempeño de seguridad, y la implementación de controles técnicos estratégicos.

Durante esta fase también lanzamos programas de concientización, establecemos procesos de gestión de vulnerabilidades, y comenzamos a integrar consideraciones de seguridad en procesos de negocio clave como adquisiciones, desarrollo de productos, y gestión de proyectos.

Fase 4: Maduración y Mejora Continua (Mes 9+)

Una vez establecidos los fundamentos, transitamos hacia un modelo de mejora continua. Esto incluye evaluaciones periódicas de efectividad de controles, ajustes al programa basados en cambios en el negocio o el panorama de amenazas, preparación para auditorías y certificaciones, y expansión de capacidades avanzadas como threat hunting, inteligencia de amenazas, y análisis predictivo de seguridad.

En esta fase, el rol de nuestro CISO evoluciona hacia uno más estratégico, enfocándose en optimización, innovación, y aseguramiento de que la seguridad habilita objetivos de negocio en lugar de obstruirlos.

Sectores que Atendemos

Sector Financiero

El sector financiero colombiano enfrenta algunos de los riesgos de ciberseguridad más significativos. Nuestros CISOs tienen experiencia profunda implementando controles que cumplen con las exigentes circulares de la Superintendencia Financiera, protegiendo sistemas de core bancario, plataformas de pagos digitales, y datos sensibles de clientes.

Entendemos los desafíos únicos de este sector: necesidad de disponibilidad 24/7, cumplimiento regulatorio estricto, sofisticación de amenazas dirigidas, y las implicaciones de reputación de cualquier brecha de seguridad.

Sector Salud

Las instituciones de salud colombianas manejan información extremadamente sensible y enfrentan requisitos únicos de disponibilidad - las vidas literalmente dependen de que los sistemas estén operacionales. Nuestros CISOs implementan programas que protegen historias clínicas electrónicas, aseguran la disponibilidad de sistemas críticos, cumplen con regulaciones de privacidad de datos de salud, y preparan a las organizaciones para amenazas específicas del sector como ransomware dirigido a hospitales.

Retail y E-commerce

El comercio digital ha experimentado un crecimiento explosivo en Colombia. Proteger plataformas de e-commerce, datos de tarjetas de pago (cumpliendo con PCI DSS), información de clientes, y sistemas de supply chain requiere expertise especializado que nuestros CISOs aportan.

Trabajamos con retailers para asegurar experiencias de compra digital que sean tanto seguras como fluidas, implementando medidas de prevención de fraude, protección contra ataques DDoS, y seguridad en aplicaciones web y móviles.

Manufactura y Logística

La convergencia de IT y OT (tecnología operacional) introduce riesgos únicos. Nuestros CISOs ayudan a organizaciones de manufactura y logística a proteger sistemas de control industrial, implementar segmentación apropiada entre redes corporativas e industriales, y desarrollar capacidades de respuesta a incidentes que consideran las particularidades de entornos OT.

Servicios Profesionales y Tecnología

Firmas de abogados, consultorías, agencias de marketing digital, y empresas de tecnología manejan información confidencial de múltiples clientes, convirtiéndolas en objetivos atractivos. Implementamos controles que protegen la confidencialidad de información de clientes, aseguran la integridad de trabajo entregado, y permiten colaboración segura con clientes y socios.

Metodologías y Frameworks que Aplicamos

Nuestro enfoque está fundamentado en las mejores prácticas de la industria global, adaptadas al contexto colombiano y las particularidades de cada cliente:

ISO/IEC 27001: Implementamos y preparamos organizaciones para la certificación en este estándar internacional de gestión de seguridad de la información, estableciendo sistemas de gestión formales, documentados y auditables.

NIST Cybersecurity Framework: Utilizamos este framework ampliamente reconocido para estructurar programas de seguridad alrededor de cinco funciones core: Identificar, Proteger, Detectar, Responder y Recuperar.

COBIT: Para alineación entre seguridad de la información y gobernanza de TI más amplia, aplicamos principios de COBIT que aseguran que las inversiones en seguridad soporten objetivos de negocio.

MITRE ATT&CK: Utilizamos este framework para modelar amenazas, diseñar controles efectivos contra tácticas y técnicas de atacantes reales, y evaluar la efectividad de capacidades de detección y respuesta.

CIS Controls: Implementamos los controles críticos de seguridad definidos por el Center for Internet Security, priorizando las "primeras acciones" más efectivas para reducir riesgos cibernéticos.

Modelo de Servicio y Engagement

Ofrecemos diferentes niveles de servicio para adaptarnos a las necesidades y presupuestos de organizaciones de diversos tamaños:

Nivel Foundational

Dirigido a pequeñas empresas o aquellas iniciando su recorrido de seguridad. Incluye 20-30 horas mensuales de CISO dedicado, suficiente para establecer políticas básicas, realizar evaluaciones trimestrales de riesgos, coordinar implementación de controles fundamentales, y proporcionar orientación estratégica a liderazgo.

Nivel Professional

Nuestro engagement más popular, apropiado para empresas medianas con operaciones digitales significativas. Incluye 40-60 horas mensuales, permitiendo gestión activa del programa de seguridad, participación en reuniones ejecutivas y de proyectos clave, gestión directa de iniciativas de seguridad, coordinación con equipos técnicos, y respuesta a incidentes cuando sea necesario.

Nivel Enterprise

Para grandes organizaciones o aquellas en sectores altamente regulados. Incluye 80-120 horas mensuales (hasta medio tiempo), proporcionando presencia regular en sitio, participación en junta directiva, gestión de equipos de seguridad internos, liderazgo de proyectos complejos, y representación de la organización ante reguladores y auditores.

Todos los niveles incluyen disponibilidad on-call para incidentes de seguridad críticos, acceso a nuestro equipo de especialistas técnicos cuando se requiere expertise adicional, y reportes regulares de métricas y desempeño del programa de seguridad.

Resultados Medibles y KPIs

Creemos en la gestión basada en datos. Establecemos indicadores clave de desempeño (KPIs) que permiten demostrar objetivamente el valor del programa de seguridad:

- **Reducción de Superficie de Ataque:** Medimos la disminución en vulnerabilidades críticas y de alto riesgo a lo largo del tiempo, con metas específicas de remediación.
- **Tiempo Promedio de Detección y Respuesta:** Cuánto tiempo transcurre entre que un incidente de seguridad ocurre y es detectado (MTTD) y cuánto tiempo toma responder efectivamente (MTTR).
- **Madurez del Programa de Seguridad:** Evaluaciones periódicas contra frameworks como CMMI o NIST, mostrando progreso mensurable en la sofisticación de capacidades de seguridad.
- **Nivel de Concientización:** Resultados de campañas de phishing simulado y evaluaciones de conocimiento, demostrando mejora en el comportamiento de seguridad de colaboradores.
- **Cumplimiento:** Porcentaje de controles implementados frente a estándares y regulaciones aplicables, con tendencia hacia cumplimiento completo.
- **Incidentes Prevenidos:** Cuantificación de amenazas bloqueadas por controles implementados, estimando el impacto financiero evitado.

Por Qué Elegir a Sisteseg

Con años de experiencia protegiendo organizaciones colombianas de todos los tamaños y sectores, Sisteseg se ha consolidado como un socio confiable en ciberseguridad. Nuestro equipo combina profundo conocimiento técnico con visión estratégica de negocio, permitiéndonos diseñar e implementar programas de seguridad que protegen efectivamente sin obstaculizar la agilidad e innovación.

Entendemos el contexto colombiano - sus regulaciones, su panorama de amenazas, sus desafíos de talent pool, y sus oportunidades. Esta comprensión local, combinada con perspectiva global de mejores prácticas, nos permite ofrecer soluciones que son tanto de clase mundial como prácticamente implementables en su organización.

Nuestro compromiso no es solo con la tecnología, sino con las personas. Invertimos en desarrollar capacidades internas en su organización, empoderando a sus equipos de TI y de negocio para que la seguridad se convierta en parte del ADN organizacional.

Testimonios de Clientes

"Antes de trabajar con Sisteseg, la seguridad era una preocupación constante pero no teníamos claridad sobre por dónde empezar. Su CISO nos ayudó a priorizar, implementar controles efectivos rápidamente, y ahora dormimos tranquilos sabiendo que tenemos un experto velando por la protección de nuestros activos digitales." - Director General, Empresa de Manufactura

"Pasar una auditoría de certificación ISO 27001 parecía una montaña imposible de escalar. El CISO de Sisteseg no solo nos guió exitosamente hacia la certificación, sino que construyó un sistema de gestión que realmente funciona para nuestra organización, no solo papeles en un archivador." - CIO, Empresa de Servicios Financieros

"Como empresa de tecnología, pensábamos que teníamos la seguridad bajo control. La evaluación inicial de Sisteseg identificó gaps críticos que no habíamos considerado. Su enfoque pragmático y orientado al negocio nos permitió fortalecer nuestra postura de seguridad sin frenar nuestra velocidad de innovación." - CEO, Startup Fintech

Cómo Empezar

Iniciar su recorrido hacia una seguridad de la información robusta con Sisteseg es simple:

1. **Contacto Inicial:** Agende una conversación sin compromiso con uno de nuestros expertos. Discutiremos sus desafíos actuales, objetivos de negocio, y cómo nuestro servicio de CISO puede apoyarlos.
2. **Evaluación Preliminar:** Realizaremos una evaluación preliminar sin costo de su postura actual de seguridad, identificando riesgos críticos y oportunidades de mejora rápida.
3. **Propuesta Personalizada:** Desarrollaremos una propuesta adaptada a su contexto específico, incluyendo nivel de servicio recomendado, roadmap inicial, estructura de costos, y expectativas de resultados.

4. **Kick-off:** Una vez acordados los términos, iniciamos inmediatamente, con su CISO asignado comenzando la evaluación detallada y planificación estratégica.

Contacto

Sisteseg - Seguridad de la Información Protegiendo el futuro digital de Colombia

Teléfono: [Número de contacto] Email: ciso@sisteseg.com Web: www.sisteseg.com

Oficinas en Bogotá | Medellín | Cali | Barranquilla

No permita que la falta de expertise interno en seguridad de la información ponga en riesgo el futuro de su organización. Con el servicio de CISO as a Service de **Sisteseg AI**, obtiene el liderazgo estratégico que necesita, cuando lo necesita, al costo que puede permitirse. Contáctenos hoy y dé el primer paso hacia una seguridad de la información verdaderamente efectiva.