

Fichas de servicio

Objetivo, alcance y forma de trabajo de cada línea.

Documento complementario al portafolio de servicios.

www.xcybershields.com info@xcybershields.com +57 321 435 3358 Bogotá, Colombia · 2026

Ficha de servicio

Threat Simulation Security Validation

Objetivo

Establecer hasta dónde puede avanzar un atacante real dentro de la organización, qué activos quedarían expuestos y cuánto tarda el equipo defensor en detectarlo y contenerlo. El resultado no es una lista teórica de riesgos, sino evidencia de lo que hoy es explotable.

Nuestro enfoque

Trabajamos bajo reglas de enfrentamiento acordadas por escrito y sobre marcos reconocidos del sector: OWASP para aplicaciones y MITRE ATT&CK para la emulación de adversarios. Cada prueba combina herramientas automatizadas con análisis manual, porque las fallas de lógica de negocio no las encuentra un escáner.

Cómo funciona

Partimos de un reconocimiento del perímetro expuesto y de la información pública de la organización. Sobre ese mapa identificamos vectores de entrada y los explotamos de forma controlada; cuando se obtiene acceso, buscamos escalar privilegios y movernos lateralmente hasta los activos objetivo. Todo el ejercicio queda registrado para que cada hallazgo pueda reproducirse y verificarse.

Alcance

- Infraestructura interna y perimetral
- Aplicaciones web, móviles y APIs
- Redes inalámbricas y accesos remotos
- Factor humano: phishing, vishing y pretexting
- Código fuente y dependencias de terceros
- Configuraciones de nube y contenedores

Beneficios

- ✓ Evidencia concreta de qué es explotable hoy y con qué grado de dificultad
- ✓ Medición real de la capacidad de detección y respuesta del equipo defensor
- ✓ Priorización de la inversión en controles según impacto verificado
- ✓ Respaldo ante requisitos de pruebas periódicas de reguladores y clientes
- ✓ Insumo técnico directo para los equipos de desarrollo y operaciones

Fases del servicio

1	2	3	4	5	6
Alcance y reglas	Reconocimiento	Identificación de vectores	Explotación controlada	Post-explotación	Cierre y verificación

Ficha de servicio

Technology Integration Cybersecurity

Objetivo

Llevar la arquitectura tecnológica a un estado seguro, operable y coherente, integrando las soluciones necesarias en cada capa sin duplicar funciones ni descartar la inversión que la organización ya realizó.

Nuestro enfoque

Partimos de lo que el cliente ya tiene. Antes de proponer una herramienta nueva revisamos qué capacidades están desaprovechadas en las licencias vigentes: con frecuencia parte de la brecha se cierra activando lo que ya se paga. Somos agnósticos frente al fabricante y elegimos según el caso de uso, no según el catálogo.

Cómo funciona

Levantamos el inventario tecnológico y lo contrastamos contra las capas de protección: usuario, endpoint, servicios y aplicaciones, conectividad y ciberseguridad. De ese contraste salen las brechas y las superposiciones. Sobre ellas definimos la arquitectura objetivo, ejecutamos la implementación por fases y acompañamos la puesta en operación y la transferencia de conocimiento al equipo interno.

Alcance

- Capa de usuario: sensibilización y concienciación
- Endpoint: antimalware, DLP, control de aplicaciones y web
- Servicios y aplicaciones: correo, WAF, CASB, DAM
- Conectividad: firewall, SD-WAN, switching y wireless
- Ciberseguridad: SIEM, SOAR, EDR/XDR y NDR
- Microsegmentación y observabilidad del entorno

Beneficios

- ✓ Una arquitectura única en lugar de herramientas sueltas que no se hablan
- ✓ Eliminación de funciones duplicadas entre productos ya adquiridos
- ✓ Menor carga operativa para el equipo interno de TI
- ✓ Despliegue por fases, sin detener la operación del negocio
- ✓ Independencia real frente al fabricante en cada decisión

Fases del servicio

1	2	3	4	5	6
Levantamiento	Análisis de brechas	Arquitectura objetivo	Implementación por fases	Puesta en operación	Transferencia

Ficha de servicio

Cyber Defense Operations

Objetivo

Reducir el tiempo que transcurre entre la entrada de una amenaza al entorno y su detección y contención, sosteniendo una capacidad de vigilancia que la mayoría de las organizaciones no puede mantener con recursos propios.

Nuestro enfoque

No monitoreamos con reglas genéricas. Construimos casos de uso sobre el contexto del cliente —sus activos críticos, sus procesos y su sector— alineados a MITRE ATT&CK, y los revisamos periódicamente para retirar los que solo generan ruido. Un SOC que produce alertas que nadie atiende no está protegiendo nada.

Cómo funciona

Integramos las fuentes de telemetría del entorno, normalizamos los eventos y los correlacionamos contra los casos de uso definidos. Cuando se dispara una alerta, un analista la valida, descarta el falso positivo o la escala según el procedimiento acordado. La respuesta se ejecuta con acciones automatizadas donde es seguro hacerlo y con intervención humana donde la decisión tiene consecuencias.

Alcance

- Monitoreo continuo de la superficie digital
- Detección basada en casos de uso a la medida
- Triaje y análisis de alertas por analistas
- Threat hunting proactivo sobre la telemetría
- Respuesta y contención de incidentes
- Inteligencia de amenazas aplicada al sector

Beneficios

- ✓ Vigilancia sostenida sin necesidad de montar un SOC propio
- ✓ Menos alertas y más señales: el ruido se depura de forma continua
- ✓ Tiempos de detección y contención medibles y comparables en el tiempo
- ✓ Escalamiento definido: se sabe quién decide qué y en qué momento
- ✓ Conocimiento del entorno que se acumula, en lugar de reiniciarse con cada incidente

Fases del servicio

1	2	3	4	5	6
Onboarding de fuentes	Casos de uso	Monitoreo continuo	Triaje y análisis	Contención y respuesta	Mejora continua

Ficha de servicio

Custom Software Development

Objetivo

Construir el software que la operación necesita y que ningún producto de catálogo resuelve, con la seguridad incorporada desde el diseño y no añadida al final como un parche.

Nuestro enfoque

Trabajamos por entregas cortas y funcionales, de modo que el cliente vea avances utilizables antes del cierre del proyecto. La seguridad entra en el ciclo de construcción —revisión de código, análisis de dependencias y controles en el despliegue— porque corregir en producción cuesta varias veces más que corregir en desarrollo.

Cómo funciona

Empezamos por entender el proceso real, no el proceso documentado: quién hace qué, dónde se pierde tiempo y qué datos se están moviendo a mano. Sobre eso definimos el alcance funcional y la arquitectura, construimos en ciclos con validación del usuario y desplegamos con pruebas automatizadas. Al cierre acompañamos la adopción y dejamos la documentación técnica para que el equipo interno pueda mantener la solución.

Alcance

- Aplicaciones web y móviles a la medida
- APIs, microservicios e integración de plataformas
- Automatización de procesos y flujos de trabajo
- Desarrollo seguro y prácticas DevSecOps
- Soluciones nativas en nube
- Modelos de inteligencia artificial y analítica

Beneficios

- ✓ Software ajustado al proceso real, sin adaptar la operación a un producto rígido
- ✓ Menos trabajo manual y menos errores de digitación entre sistemas
- ✓ Vulnerabilidades corregidas en desarrollo, donde son más baratas
- ✓ Avances utilizables durante el proyecto y no solo al final
- ✓ Documentación y transferencia para no quedar atado al proveedor

Fases del servicio

1	2	3	4	5	6
Descubrimiento	Alcance y arquitectura	Construcción por ciclos	Pruebas y seguridad	Despliegue	Adopción y soporte

Ficha de servicio

Cyber Resilience Consulting

Objetivo

Dotar a la organización de una estructura de gobierno, cumplimiento y continuidad que le permita tomar decisiones de seguridad con criterio y sostener la operación cuando algo falle.

Nuestro enfoque

Adaptamos el marco a la organización y no al revés. Una política que nadie puede cumplir no reduce riesgo, solo genera evidencia de incumplimiento. Por eso escribimos documentos aplicables, dimensionados al tamaño y la madurez real del cliente, y validados con quienes van a ejecutarlos.

Cómo funciona

Evaluamos el estado actual frente al marco de referencia acordado —ISO 27001, NIST u otro aplicable — y lo traducimos en un mapa de brechas con su nivel de criticidad. De ahí sale una hoja de ruta priorizada con horizontes definidos. En paralelo desarrollamos las políticas y procedimientos faltantes y construimos los planes de continuidad y recuperación, que se prueban antes de darse por cerrados.

Alcance

- Evaluación de riesgo cibernético del negocio
- Diagnóstico de brechas frente a ISO 27001
- Medición de madurez y su evolución en el tiempo
- Gobierno, cumplimiento y estructura de responsabilidades
- Políticas y procedimientos aplicables
- Planes de continuidad (BCP) y recuperación (DRP)

Beneficios

- ✓ Un criterio claro para decidir en qué invertir primero y por qué
- ✓ Preparación ordenada frente a auditorías, clientes y reguladores
- ✓ Planes de continuidad probados y no solo redactados
- ✓ Responsabilidades asignadas: se sabe quién responde ante cada escenario
- ✓ Un punto de partida medible contra el cual comparar el avance

Fases del servicio

1	2	3	4	5	6
Diagnóstico inicial	Análisis de brechas	Hoja de ruta	Desarrollo normativo	Continuidad y recuperación	Pruebas y ajuste

Ficha de servicio

Cloud AI Transformation

Objetivo

Llevar las cargas de trabajo a la nube con la arquitectura, el control de costos y la seguridad correctas desde el inicio, y habilitar sobre ella las capacidades de inteligencia artificial que el negocio pueda aprovechar.

Nuestro enfoque

Migrar no es mover servidores de sitio. Revisamos carga por carga si conviene rehospedar, rediseñar o dejar donde está, porque una migración mal planteada termina costando más que el centro de datos que reemplaza. La configuración segura y el control de gasto se definen antes del primer despliegue, no después de la primera factura.

Cómo funciona

Inventariamos las cargas y sus dependencias, y definimos para cada una la estrategia de migración y el modelo de servicio adecuado. Diseñamos la arquitectura objetivo en Azure o AWS con identidades, redes y controles de acceso definidos, migramos por olas con ventanas acordadas y optimizamos consumo y rendimiento una vez en operación.

Alcance

- Arquitectura y despliegue en Microsoft Azure
- Arquitectura y despliegue en Amazon Web Services
- Modelos IaaS y PaaS según cada carga
- Migración planificada de aplicaciones y datos
- Seguridad, identidades y control de accesos en nube
- DevOps, automatización y esquemas híbridos

Beneficios

- ✓ Decisión razonada carga por carga, no una migración en bloque
- ✓ Costos bajo control desde el diseño y no como sorpresa mensual
- ✓ Configuración segura por defecto en lugar de corrección posterior
- ✓ Capacidad de escalar con la demanda sin rediseñar la arquitectura
- ✓ Base técnica lista para incorporar analítica e inteligencia artificial

Fases del servicio

1	2	3	4	5	6
Inventario de cargas	Estrategia de migración	Arquitectura objetivo	Migración por olas	Aseguramiento	Optimización

Ficha de servicio

Cyber Risk & Third-Party Risk Management

Objetivo

Traducir el riesgo cibernético a cifras financieras que el comité directivo pueda comparar con cualquier otro riesgo del negocio, y extender esa misma medición a los terceros de los que depende la operación.

Nuestro enfoque

Una matriz de colores no permite decidir un presupuesto. Cuantificamos la exposición en términos económicos, con supuestos explícitos y trazables, de modo que cualquiera pueda discutir el modelo y no solo aceptar el resultado. En terceros aplicamos un esfuerzo proporcional a la criticidad: no todos los proveedores merecen la misma profundidad.

Cómo funciona

Identificamos los escenarios de pérdida relevantes para el negocio y estimamos frecuencia e impacto con la información disponible de la organización y del sector. Sobre esa base calculamos la exposición, evaluamos qué reducción aporta cada control candidato y construimos la comparación de retorno. El mismo ejercicio se aplica a la cartera de proveedores, clasificada por criticidad.

Alcance

- Cuantificación del riesgo en métricas financieras
- Medición del retorno de la inversión en controles (ROSI)
- Priorización por impacto económico y reducción de riesgo
- Clasificación de proveedores por criticidad
- Evaluación y seguimiento del riesgo de terceros
- Reportes ejecutivos para junta y comités

Beneficios

- ✓ Un lenguaje común entre el área de seguridad, la financiera y la junta
- ✓ Sustento numérico para defender o descartar una inversión en controles
- ✓ Visibilidad del riesgo que entra por la cadena de suministro
- ✓ Requisitos de seguridad definidos antes de firmar con un tercero
- ✓ Seguimiento de la exposición a lo largo del tiempo y no una foto aislada

Fases del servicio

1	2	3	4	5	6
Escenarios de pérdida	Recolección de datos	Modelo de cuantificación	Evaluación de controles	Análisis de terceros	Reporte ejecutivo

Ficha de servicio

IT Infrastructure Video Surveillance System

Objetivo

Sostener la infraestructura tecnológica que soporta la operación diaria y proteger las instalaciones y los activos físicos con sistemas de videovigilancia integrados al resto del entorno tecnológico.

Nuestro enfoque

Tratamos la infraestructura y la videovigilancia como parte de la misma superficie de riesgo. Una cámara conectada a la red es un dispositivo más que hay que segmentar, actualizar y monitorear; instalarla sin ese criterio abre una puerta en lugar de cerrarla. El mantenimiento preventivo se programa, no se improvisa cuando algo falla.

Cómo funciona

Evaluamos el estado del parque tecnológico y de las instalaciones, y definimos el dimensionamiento necesario según crecimiento previsto y puntos a cubrir. Implementamos la infraestructura y el sistema de videovigilancia con la segmentación de red correspondiente, y operamos el mantenimiento bajo un calendario preventivo con atención correctiva y niveles de servicio acordados.

Alcance

- Diseño e implementación de infraestructura de TI
- Outsourcing y operación de la infraestructura
- Mantenimiento preventivo y correctivo programado
- Videovigilancia con analítica y alta definición
- Acceso remoto y almacenamiento local, nube o híbrido
- Segmentación e integración con el entorno existente

Beneficios

- ✓ Disponibilidad sostenida de los sistemas que soportan la operación
- ✓ Fallas prevenidas antes de convertirse en interrupciones
- ✓ Mayor vida útil del equipamiento ya instalado
- ✓ Cobertura física y digital gestionada bajo un mismo criterio
- ✓ Un solo interlocutor para infraestructura, seguridad y soporte

Fases del servicio

1	2	3	4	5	6
Evaluación del entorno	Dimensionamiento	Diseño de solución	Implementación	Puesta en marcha	Operación y mantenimiento

Hablemos

Conversemos su caso

Cada una de estas fichas describe cómo trabajamos el servicio en general. El alcance definitivo, los tiempos y el modelo de entrega se definen sobre la realidad de su organización.



Correo

info@xcybershields.com

Teléfono

+57 321 435 3358

Sitio web

www.xcybershields.com

XCYBERSHIELDS S.A.S.

Bogotá D.C., Colombia

Expertos en tu escudo digital.