operasec

DOSSIER DE PRESENTACIÓN

ÍNDICE

Seleccione una sección para acceder directamente al contenido.

Qué es Operasec

Seguridad de la información, dispositivos reforzados y servicios técnicos especializados

Operasec es una marca técnica especializada en seguridad de la información, dispositivos seguros y reforzados, y servicios técnicos para entornos profesionales.

La actividad de Operasec se centra en preparar soluciones orientadas a mejorar la seguridad, la privacidad, la verificabilidad y el control técnico de dispositivos, redes y entornos profesionales. El enfoque no es solo facilitar el uso diario, sino ofrecer tecnología preparada con criterios de seguridad de la información, transparencia técnica y reducción de superficie de exposición.

Operasec trabaja en varias áreas complementarias: preparación de dispositivos seguros, configuración de redes protegidas, despliegues empresariales, revisión técnica de entornos, servicios TSCM, salas seguras y análisis técnico de móviles, portátiles y equipos informáticos.

La diferencia está en el enfoque personalizado. No trabajamos con configuraciones genéricas ni con soluciones cerradas. Cada dispositivo, red o intervención se prepara según el perfil del cliente, su entorno de uso, las aplicaciones necesarias, el nivel técnico del usuario y las medidas de seguridad adecuadas para su actividad.

En el área de productos, Operasec prepara teléfonos, tablets, portátiles, estaciones de trabajo, routers, firewalls y llaves de autenticación con configuraciones adaptadas al cliente. Estos dispositivos pueden incluir sistemas reforzados, firmware verificable, cifrado, control de permisos, VPN, firewall, perfiles separados, aplicaciones listas para usar, MDM o administración centralizada cuando procede, y soporte posterior.

En el área de servicios, Operasec ofrece revisión técnica de espacios profesionales, barridos electrónicos TSCM, blindaje de salas de reuniones y análisis técnico de dispositivos ante indicios de software malicioso, accesos no autorizados, manipulación o necesidad de verificación.

Áreas de trabajo

Dos líneas principales

Productos seguros y reforzados

Teléfonos, tablets, portátiles, estaciones de trabajo, routers/firewalls y llaves de autenticación preparados para ofrecer mayor seguridad, privacidad y control técnico.

Esta línea incluye OperaPhone, OperaTablet, OperaPad, OperaPC, OperaWall y OperaKey, además de despliegues empresariales, administración centralizada, MDM o sistemas equivalentes cuando el tipo de dispositivo lo permite.

Servicios técnicos especializados

Servicios profesionales orientados a la revisión, protección y verificación técnica de entornos y dispositivos.

Esta línea se divide en tres servicios principales:

- **Servicio TSCM:** barridos electrónicos profesionales para detectar, localizar y documentar posibles dispositivos de escucha, grabación, transmisión o seguimiento no autorizados en oficinas, despachos, salas de reuniones, vehículos y otros entornos profesionales.
- **Servicio de blindaje:** blindaje de salas de reuniones y ambientes profesionales.
- **Servicio de análisis técnico de dispositivos electrónicos:** revisión de móviles, portátiles, ordenadores y otros equipos ante indicios de software malicioso, accesos no autorizados, manipulación o necesidad de verificación.

A quién va dirigido

Empresas, despachos y profesionales que necesitan seguridad clara y verificable

Operasec está orientada a clientes que valoran la discreción, la transparencia técnica y la posibilidad de revisar las medidas aplicadas.

Perfiles habituales

- empresas y grupos empresariales;
- despachos de abogados y asesorías profesionales;
- equipos directivos y alta dirección;
- departamentos jurídicos, financieros o estratégicos;
- consultoras y firmas profesionales;
- profesionales con alta responsabilidad sobre documentación, comunicaciones o dispositivos;
- periodistas y perfiles profesionales expuestos;
- particulares con necesidades avanzadas de seguridad y privacidad;
- clientes que necesitan mejorar la seguridad de dispositivos, redes o salas de reuniones.

Nuestra diferencia

Soluciones preparadas, no productos genéricos

La diferencia de Operasec está en la preparación individual. No entregamos únicamente un dispositivo, una herramienta o una intervención aislada: preparamos una solución adaptada al uso real del cliente.

Seguridad de la información

Reforzamos dispositivos, comunicaciones, accesos, redes y espacios profesionales mediante medidas técnicas claras, documentadas y revisables.

Dispositivos listos para trabajar

Los equipos pueden entregarse con sistema operativo, aplicaciones, VPN, firewall, cifrado, perfiles, permisos, comunicaciones, actualizaciones y políticas de seguridad configuradas.

Tecnología verificable

Priorizamos firmware verificable, sistemas revisables, arranque verificado, cifrado, control de permisos, reducción de superficie de ataque y configuraciones que puedan ser comprobadas por el cliente o por su equipo técnico.

Soporte y acompañamiento

Operasec acompaña al cliente antes de la entrega, durante la preparación y después del uso inicial, resolviendo dudas y ajustando configuraciones cuando procede.

Red técnica especializada

Cuando el proyecto lo requiere, Operasec puede apoyarse en colaboradores técnicos, peritos informáticos, especialistas TSCM y profesionales cualificados.

Hardware seguro y verificable

Seguridad, privacidad y facilidad de uso

Los productos de Operasec siguen una filosofía sencilla: dispositivos preparados para ofrecer mayor seguridad, transparencia técnica y control sobre el entorno de trabajo.

Cada dispositivo puede configurarse a medida, con aplicaciones, servicios, políticas de seguridad y soporte adaptados al cliente.

OperaPhone

Teléfono móvil seguro y reforzado para comunicaciones profesionales

OperaPhone es un teléfono preparado para clientes que necesitan un entorno móvil más seguro, privado y auditable.

Puede incluir borrado remoto, borrado por intentos fallidos, bloqueo ante tirón o movimiento brusco, PIN anti coacción, control USB, firewall avanzado, VPN, licencia de Threema, ecosistema Proton opcional, aplicaciones instaladas, servicios de Google opcionales y aislados, MDM auditable y opción de inhabilitar por completo cualquier SMS entrante, reduciendo la exposición asociada al número de teléfono, una vía habitual en intentos de infección por spyware y otras amenazas cibernéticas.

Su base técnica combina hardware Pixel moderno, chip Titan M2, cifrado completo, arranque verificado, aislamiento de aplicaciones, permisos granulares, perfiles separados, control de sensores, reducción de telemetría, control USB y actualizaciones frecuentes.

Opcionalmente, OperaPhone puede entregarse con componentes físicos retirados a petición del cliente, como cámaras, micrófonos, altavoces o sensores, entregando dichos componentes aparte. Esta opción permite reducir físicamente determinadas superficies de riesgo, no solo desactivar funciones por software.

OperaTablet

Tablet segura para movilidad, reuniones y documentación

OperaTablet ofrece la filosofía de OperaPhone en formato tablet: seguridad, facilidad de uso, pantalla amplia y entorno preparado para trabajar.

Está orientada a reuniones, consulta documental, movilidad empresarial, videoconferencias, presentaciones internas y acceso a herramientas corporativas.

Puede incluir borrado remoto, borrado por intentos fallidos, PIN anti coacción, bloqueo ante tirón o movimiento brusco, control USB, VPN, firewall, aplicaciones instaladas, ecosistema Proton opcional, servicios de Google opcionales y aislados, perfiles separados y MDM auditable.

Puede basarse en hardware Pixel Tablet, con Titan M2, cifrado completo, arranque verificado, aislamiento de aplicaciones, permisos granulares, control de cámara, micrófono, ubicación y sensores, reducción de telemetría y actualizaciones frecuentes durante el ciclo de soporte.

OperaPad

Portátil seguro para movilidad y trabajo profesional

OperaPad es la línea de portátiles seguros de Operasec. Está pensado para viajes, reuniones, trabajo fuera de la oficina y entornos donde el equipo puede estar más expuesto físicamente.

Su base técnica se apoya en hardware seleccionado para admitir firmware verificable como Dasharo/Coreboot, Coreboot o Libreboot, según la versión elegida. Puede incluir Intel Management Engine desactivado o neutralizado, cifrado completo del disco, arranque medido, Heads, verificación anti-manipulación y llave física de comprobación.

OperaPad puede configurarse con Qubes OS, Ubuntu LTS, Debian, Linux Mint u otros sistemas compatibles. Qubes OS permite separar áreas de trabajo mediante entornos independientes; Ubuntu, Debian o Linux Mint ofrecen una experiencia más sencilla, estable y fácil de mantener.

Cada OperaPad se entrega preparado según el caso del cliente, con VPN, firewall, DNS seguro, navegador endurecido, gestor de contraseñas, ecosistema Proton opcional, herramientas corporativas, aplicaciones del cliente, políticas de seguridad, documentación de configuración y soporte posterior.

Opcionalmente, puede añadirse sellado físico o medidas de control para dificultar o evidenciar manipulaciones durante transporte, almacenamiento o ausencia del usuario.

OperaPC

Estación de trabajo segura, verificable y de alto rendimiento

OperaPC es una estación de trabajo segura para puestos fijos, despachos, oficinas y entornos donde se necesita más rendimiento, estabilidad y control técnico que en un equipo convencional.

Su base técnica se apoya en hardware actual de alto rendimiento, con procesadores modernos, memoria RAM rápida, almacenamiento NVMe y componentes seleccionados por estabilidad, potencia y compatibilidad con configuraciones reforzadas.

Puede incluir firmware verificable como Dasharo/Coreboot, Coreboot o Libreboot, según la versión elegida. Dasharo puede configurarse con Heads para arranque medido y verificación anti-manipulación, o con UEFI/TianoCore para clientes que priorizan compatibilidad amplia y facilidad de uso.

OperaPC puede entregarse con Intel Management Engine desactivado o neutralizado, cifrado completo del disco, verificación mediante llave física de comprobación, Qubes OS, Ubuntu LTS, Debian, Linux Mint u otros sistemas compatibles.

Se entrega preparado según el caso del cliente, con VPN, firewall, DNS seguro, navegador endurecido, gestor de contraseñas, ecosistema Proton opcional, herramientas corporativas, aplicaciones del cliente, políticas de seguridad, configuración documentada y soporte posterior.

Opcionalmente, puede añadirse sellado físico de la carcasa para dificultar o evidenciar manipulaciones durante transporte, almacenamiento o ausencia del usuario.

OperaWall

Firewall, gateway VPN y seguridad de red profesional

OperaWall es la línea de routers, gateways y firewalls seguros de Operasec, orientada a oficinas, despachos profesionales, puestos de trabajo sensibles y entornos donde se necesita una red más controlada.

Puede funcionar como firewall profesional, sistema de prevención de intrusiones IPS y gateway VPN, con configuraciones basadas en OPNsense u OpenWrt según el caso de uso. Permite aplicar reglas de filtrado, segmentación de red, control de tráfico, VPN, DNS seguro, autenticación reforzada y políticas de acceso para equipos de trabajo.

Su base técnica puede incluir firmware verificable Dasharo Coreboot UEFI, orientado a transparencia técnica, menor superficie de ataque y arranque rápido. A nivel hardware, puede configurarse sobre equipos compactos de alto rendimiento con CPU Intel, AES-NI para tráfico VPN, memoria RAM suficiente, almacenamiento NVMe y puertos Ethernet de alta velocidad.

OperaWall puede prepararse como firewall para oficina o despacho, router de viaje, gateway VPN, punto de acceso WiFi, solución con conexión LTE/4G de respaldo o equipo de red para entornos donde se requiere alta disponibilidad y control técnico.

Según las necesidades del cliente, también puede configurarse con otros sistemas compatibles como pfSense, Ubuntu, Windows o Proxmox, pudiendo funcionar como firewall, router avanzado, gateway seguro o equipo compacto de uso técnico.

OperaWall se entrega listo para usar, con servidores, credenciales, reglas de red, VPN, políticas de acceso y configuración documentada según el entorno del cliente.

OperaKey

Llaves físicas de autenticación listas para usar

OperaKey es la línea de llaves físicas de autenticación preparadas por Operasec para proteger accesos críticos, cuentas corporativas y servicios compatibles con FIDO2, passkeys, WebAuthn y autenticación multifactor.

Estas llaves permiten iniciar sesión mediante un dispositivo físico, reduciendo de forma importante el riesgo de phishing, robo de contraseñas, suplantación de identidad y accesos no autorizados. Son especialmente útiles en empresas y despachos donde varios empleados acceden a correo corporativo, servicios cloud, gestores de contraseñas, paneles administrativos, herramientas internas o cuentas con permisos elevados.

OperaKey se prepara con llaves físicas compatibles seleccionadas según las necesidades técnicas del cliente, el entorno de uso y los
servicios que se deseen proteger.

Utilidades principales

- protección frente a phishing y páginas falsas de inicio de sesión;
- autenticación fuerte en correo corporativo, servicios cloud y herramientas internas;
- protección de gestores de contraseñas y cuentas administrativas;
- uso con passkeys, FIDO2, WebAuthn y doble factor de autenticación;
- reducción del riesgo asociado a contraseñas débiles, reutilizadas o filtradas;
- despliegue para empleados, socios, directivos o personal con acceso a sistemas críticos;
- llaves de respaldo para recuperación segura de cuentas;
- configuración inicial, guía de uso y recomendaciones de custodia.

Operasec puede entregar las llaves configuradas, documentadas y acompañadas de recomendaciones prácticas para su uso diario. En despliegues empresariales, puede ayudar a definir qué cuentas proteger primero, cuántas llaves utilizar por usuario, cómo custodiar llaves de respaldo y cómo reducir errores habituales en la implantación de autenticación fuerte.

Despliegues para empresas y despachos

Configuración homogénea, administración y soporte

Operasec puede preparar despliegues para una persona, un equipo directivo, un despacho o una empresa que necesita una configuración coherente en varios dispositivos.

Los productos pueden integrarse en despliegues con políticas de configuración, administración centralizada, MDM o sistemas equivalentes cuando el tipo de dispositivo lo permite.

Ejemplos de despliegue

- OperaPhones para socios, directivos o personal con necesidad de comunicaciones reforzadas;
- OperaTablets para reuniones, consulta documental o movilidad empresarial;
- OperaPads para trabajo fuera de la oficina, documentación profesional o viajes;
- OperaPC para puestos fijos reforzados;
- OperaKeys para proteger accesos críticos y cuentas corporativas;
- OperaWall para segmentar y proteger redes de trabajo;
- políticas de seguridad, soporte y documentación adaptadas al cliente.

Servicios TSCM

Barridos electrónicos y revisión técnica de espacios profesionales

Operasec ofrece servicios TSCM en España y Portugal para revisar salas, despachos, oficinas, vehículos y entornos donde se tratan conversaciones, documentación o decisiones de importancia para el cliente.

Los barridos electrónicos pueden realizarse por peritos judiciales en TSCM y especialistas con experiencia, empleando equipos profesionales de referencia en el sector. Cuando el caso lo requiere, el servicio puede acompañarse de documentación técnica o informe pericial.

Ámbitos de revisión

- salas de reuniones;
- despachos de dirección;
- oficinas;
- vehículos;
- domicilios profesionales;
- zonas de archivo o documentación;
- teléfonos fijos y sistemas de comunicación;
- equipos eléctricos o electrónicos que deban revisarse;
- mobiliario, objetos instalados, redes y puntos de conexión expuestos.

Elementos que pueden detectarse o revisarse

- micrófonos ocultos;
- cámaras ocultas;
- grabadoras autónomas;
- transmisores analógicos o digitales;
- dispositivos GSM, WiFi, Bluetooth u otros sistemas de transmisión;
- localizadores GPS;
- dispositivos conectados a alimentación eléctrica;
- manipulaciones físicas visibles;
- elementos no autorizados en espacios profesionales.

Equipamiento y enfoque técnico

Se utilizan equipos profesionales de fabricantes especializados como REI y MEFF, incluyendo herramientas de análisis de radiofrecuencia, detección de transmisiones, inspección de líneas, detección de dispositivos electrónicos ocultos y revisión técnica de entornos profesionales.

El equipamiento puede incluir soluciones de referencia como REI ORION, REI TALAN, MEFF M1-PRO, MEFF M2-PRO y otros equipos profesionales de última generación de REI y MEFF.

Blindaje de espacios profesionales

Espacios preparados para reuniones profesionales

Operasec puede asesorar en la creación, mejora o preparación de salas de reuniones para empresas y despachos que necesitan un entorno más controlado para conversaciones, documentación y decisiones relevantes.

Una sala segura combina diseño físico, control de dispositivos, procedimientos de uso, revisión técnica, privacidad acústica, control de comunicaciones y hábitos adecuados del personal.

Elementos que pueden considerarse

- evaluación inicial del espacio;
- control de accesos;
- gestión de dispositivos móviles antes de reuniones;
- revisión de mobiliario y elementos electrónicos;
- protección acústica o enmascaramiento sonoro;
- control de redes inalámbricas;
- revisión de cableado y puntos de conexión;
- bloqueadores de micrófonos o sistemas de protección acústica según el entorno;
- estudio de apantallamiento o jaula de Faraday en casos de alta exigencia;
- monitorización o revisión del espectro radioeléctrico cuando el contexto lo justifique;
- protocolos de uso antes, durante y después de reuniones.

Cada proyecto se adapta al espacio, presupuesto, urgencia y nivel de revisión requerido.

Análisis técnico de dispositivos

Móviles, portátiles y equipos informáticos

Operasec ofrece análisis técnico de dispositivos móviles, portátiles y equipos informáticos ante comportamientos anómalos, indicios de software malicioso, accesos no autorizados, manipulación, pérdida de control del sistema o necesidad de revisión técnica.

El análisis se hace con apoyo de peritos informáticos colaboradores y, cuando el cliente lo necesita, acompañarse de informe técnico o pericial.

El análisis puede orientarse a revisar

- aplicaciones sospechosas;
- conexiones anómalas;
- persistencia no autorizada;
- configuraciones inseguras;
- exposición de credenciales;
- indicios de manipulación;
- actividad anómala;
- riesgos derivados de servicios instalados

Transparencia y confianza

Medidas revisables y documentación clara

Operasec trabaja con un enfoque transparente. La seguridad no depende de promesas absolutas, sino de buenas decisiones técnicas, configuración adecuada, mantenimiento, hábitos de uso y revisión cuando procede.

Nuestras soluciones se basan en:

- tecnologías verificables;
- configuraciones documentadas;
- cifrado y separación de entornos;
- reducción de superficie de ataque;

- control de permisos, red y aplicaciones;
- actualizaciones frecuentes;
- revisión por el cliente, su equipo técnico o peritos de confianza;
- soporte y acompañamiento posterior.

El objetivo es que el cliente entienda qué se ha preparado, qué riesgos se reducen y cómo debe utilizar la solución para mantener un buen nivel de protección.

Tecnología preparada para trabajar con mayor seguridad y confianza

Operasec combina dispositivos seguros y reforzados, despliegues profesionales, servicios TSCM, análisis técnico de dispositivos y blindaje de entornos de trabajo más controlados.

Nuestra diferencia está en el trato personalizado: cada teléfono, tablet, portátil, estación de trabajo, red, sala o intervención se prepara según el cliente, no según una plantilla genérica.

Operasec
Seguridad de la información · Dispositivos reforzados · Servicios técnicos especializados
TSCM · Salas seguras · Análisis técnico

Contacto:

Web: www.operasec.com

Email: info@operasec.com

Teléfono: (consultar por email)