General Protec CiberSafe

Servicio de Ciberseguridad Permanente y Gestionada

CiberSafe, de General Protec, es un servicio de ciberseguridad permanente diseñado para las pymes que necesitan una protección robusta, intuitiva y rentable. En un entorno donde las amenazas evolucionan constantemente, CiberSafe ofrece la tranquilidad de contar con una defensa siempre activa, gestionada por un equipo de expertos que vela por su seguridad sin descanso.

Disfrute de la confianza de operar en el mundo digital sabiendo que su información, sus datos y su identidad están protegidos por una solución integral que combina tecnología de última generación con supervisión humana experta.

Principales beneficios de CiberSafe:

1. Protege su negocio contra malwares, virus, phishing, ransomware, etc...

2. La monitorización 24/7 y la respuesta inmediata evitan que los incidentes paralicen su empresa.

3. Su técnico dedicado gestiona la seguridad, permitiéndole centrarse en su negocio.

4. Convierte la ciberseguridad en una ventaja competitiva tangible y certificada.

Asignación de un Técnico Dedicado, Cuestionario Inicial y Auditoría

A cada cliente se le asigna un técnico dedicado. A partir de un cuestionario inicial y una auditoría, el técnico conocerá su infraestructura, actuará como su punto de contacto directo monitorizando su entorno digital 24/7 y responderá de inmediato para neutralizar cualquier amenaza.

Instalación de la Suite de Ciberseguridad CiberComplet

El técnico dedicado instala la suite CiberComplet de forma remota en los diferentes equipos. Esta suite incluye anti-malware con escáner de doble motor. Protección multicapa en tiempo real, antivirus, cortafuegos, bloqueador de comportamiento, prevención de exploits, prevención de ataques dirigidos incluido el spear-phishing, el malware de un solo uso, protección contra malware sin archivos, protección web, anti-phishing y anti-ransomware.

Formación y Certificación

Incluimos el programa CiberTraining para concienciar a los usuarios, convirtiendo el factor humano en una línea de defensa. Al finalizar la implementación, le entregamos un certificado conforme cumple los requisitos de la norma ISO 27032, un valor tangible para sus clientes y socios.

Requisitos CiberComplet:

- Sistemas Operativos: Windows, macOS
- Recursos: Agente ligero de bajo consumo, optimizado para no afectar al rendimiento del equipo.
- Conexión a Internet: Requerida para la monitorización y actualización en tiempo real.

Qué incluye CiberSafe:

- Licencia de la Suite de Seguridad CiberComplet
- Servicio de Técnico Dedicado y Monitorización SOC 24/7
- Auditoría Inicial de Ordenadores y Vulnerabilidades Web (CiberAuditWeb)
- Programa de Formación para Empleados (CiberTraining)
- Certificado de cumplimiento de requisitos de la norma ISO 27032

Qué incluye General Protec CiberSafe:

Características	Acción	Cómo protege
Técnico Dedicado y SOC 24/7	Monitoriza, analiza y responde a incidentes de seguridad de forma ininterrumpida.	Le libera de la gestión de alertas y garantiza una respuesta experta e inmediata, asegurando la continuidad de su negocio.
Protección Multicapa en Tiempo Real	Combina diversas tecnologías de seguridad (firmas, comportamiento, web, etc.) que operan simultáneamente.	Crea una defensa profunda y resiliente. Si una amenaza logra eludir una capa, es detectada y bloqueada por la siguiente.
Detección de Virus y Malware de Doble Motor	Utiliza dos motores de escaneo coordinados para maximizar la detección de todo tipo de malware (virus, troyanos, spyware, etc.).	Aumenta la tasa de detección y la velocidad del escaneo, ofreciendo una protección más completa y eficiente contra software malicioso.
Bloqueador de Comportamiento	Monitoriza las acciones y el comportamiento de todos los programas en ejecución en tiempo real.	Detecta y detiene amenazas nuevas y de día cero (zero-day) basándose en su conducta maliciosa, no en firmas de virus conocidas.
Anti-Ransomware	Detecta y bloquea los procesos de ransomware antes de que comiencen a cifrar archivos.	Asegura la integridad y disponibilidad de los datos, previniendo el secuestro de información y la extorsión cibernética.
Anti-Phishing y Protección Web	Bloquea el acceso a nivel de host a sitios web maliciosos, fraudulentos o de suplantación de identidad conocidos.	Evita el robo de credenciales y el fraude online al neutralizar la amenaza antes de que el usuario pueda interactuar con la página falsa.
Protección contra Malware sin Archivos	Utiliza una combinación de tecnologías para detectar código malicioso que se ejecuta directamente en la memoria del sistema.	Detiene una de las técnicas de ataque más evasivas y modernas, que los antivirus tradicionales no pueden detectar al no haber un archivo que escanear.
Prevención de Exploits	Detecta y bloquea las técnicas utilizadas para explotar vulnerabilidades de software antes de que puedan ejecutar código malicioso.	Protege contra ataques que se aprovechan de fallos de seguridad en programas no actualizados, incluso antes de que exista un parche.
Endurecimiento de la Aplicación	Impide que aplicaciones legítimas (como MS Office, navegadores) ejecuten acciones peligrosas o scripts maliciosos.	Cierra una vía de ataque común, donde los delincuentes explotan vulnerabilidades en software confiable para ejecutar código dañino.
Prevención de Manipulación del Sistema	Alerta y bloquea cambios no autorizados en áreas críticas del sistema operativo y de las aplicaciones.	Impide que el malware establezca persistencia en el sistema, modifique su configuración de seguridad o redirija el tráfico de internet.
Protección Avanzada contra Amenazas Persistentes (APT)	Combina múltiples capas de detección para identificar las tácticas sigilosas y a largo plazo utilizadas por los atacantes avanzados.	Detecta y neutraliza ataques complejos y dirigidos que intentan permanecer ocultos en la red durante largos períodos para robar información.
Prevención de Ataques Dirigidos	Combina la detección de comportamiento y la heurística para identificar ataques diseñados específicamente para una organización.	Ofrece defensa contra las amenazas más peligrosas y personalizadas, como el ciberespionaje industrial o el spear-phishing.

Requisitos CiberComplet:

- Sistemas Operativos: Windows, macOS
- Recursos: Agente ligero de bajo consumo, optimizado para no afectar al rendimiento del equipo.
- Conexión a Internet: Requerida para la monitorización y actualización en tiempo real.

Qué incluye CiberSafe:

- Licencia de la Suite de Seguridad CiberComplet
- Servicio de Técnico Dedicado y Monitorización SOC 24/7
- Auditoría Inicial de Ordenadores y Vulnerabilidades Web (CiberAuditWeb)
- Programa de Formación para Empleados (CiberTraining)
- Certificado de cumplimiento de requisitos de la norma ISO 27032

Qué incluye General Protec CiberSafe:

Características	Acción	Cómo protege
Protección de Botnet	Impide que el malware tome el control del dispositivo y lo incorpore a una red de bots.	Evita que los recursos de su equipo sean utilizados para fines delictivos, como lanzar ataques DDoS o enviar spam.
Guardia de Archivo	Escanea en tiempo real cada archivo que se descarga, modifica o ejecuta en el sistema.	Proporciona una defensa constante y automática, asegurando que ningún archivo malicioso pueda activarse en el dispositivo.
Limpieza Avanzada de Infecciones	Realiza una desinfección profunda del sistema, revisando y restaurando más de 70 puntos de ejecución automática y áreas críticas.	Asegura la eliminación completa y segura de malware persistente (rootkits) y repara el daño causado al sistema operativo.
Seguridad del Navegador	Proporciona una extensión para los principales navegadores (Chrome, Firefox, Edge) que bloquea el acceso a URLs maliciosas.	Añade una capa de seguridad adicional y consciente de la privacidad directamente en el navegador, sin rastrear el historial del usuario.
Escaneos del Sistema Súper Rápidos	Realiza un análisis completo del dispositivo en un tiempo muy reducido (típicamente 1-2 minutos).	Permite realizar revisiones de seguridad frecuentes sin afectar a la productividad del usuario, garantizando una detección temprana.
Cuarentena Segura de Archivos Sospechosos	Aísla y cifra el malware detectado en un entorno seguro de cuarentena.	Impide que el archivo malicioso cause daño alguno al sistema, permitiendo su análisis seguro por parte de los técnicos.
Modo de Bloqueo de Red de Emergencia	Realiza un análisis completo del dispositivo en un tiempo muy reducido (típicamente 1-2 minutos).	Permite realizar revisiones de seguridad frecuentes sin afectar a la productividad del usuario, garantizando una detección temprana.
Verificación de Falsos Positivos	Compara las detecciones con un servicio de reputación global en la nube antes de tomar una acción definitiva.	Asegura la máxima precisión, evitando interrupciones innecesarias del trabajo al no bloquear aplicaciones legítimas por error.
Exclusiones de Protección / Lista de Permitidos	Permite configurar excepciones para archivos, carpetas o programas confiables para que no sean analizados.	Asegura la compatibilidad con software empresarial específico, evitando falsos positivos y interrupciones en el flujo de trabajo.
CiberTraining	Forma y conciencia a los empleados sobre las mejores prácticas en ciberseguridad.	Fortalece el eslabón más vulnerable, el humano, reduciendo drásticamente el riesgo de incidentes causados por error.

General Protec

www.generalprotec.com/cibersafe

ISO 27032