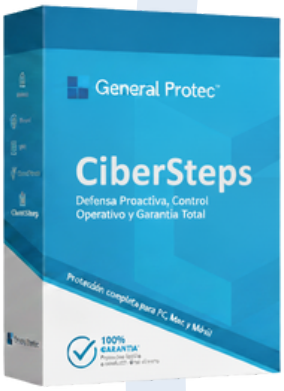

General Protec CiberSteps

Defensa Proactiva, Control Operativo y Garantía Total

CiberSteps, de General Protec, es la solución de élite para organizaciones con tolerancia cero al riesgo. No solo ofrece una defensa impenetrable, sino que integra la ciberseguridad con la gestión estratégica de TI. Esta suite trabaja de forma proactiva para identificar y neutralizar amenazas antes de que afecten a la integridad del negocio, garantizando la máxima resiliencia.

Principales beneficios de CiberSteps:

1. Anticipa amenazas avanzadas: Caza y neutraliza ataques sofisticados con EDR, Inteligencia Artificial y Sandbox.

2. Optimiza la infraestructura de TI: Gestiona y automatiza el mantenimiento de sus sistemas para reducir vulnerabilidades y prevenir fallos.

3. Elimina el riesgo financiero: Nuestra Garantía CiberSteps asegura su inversión, reembolsando tres veces la cuota anual en caso de un ataque exitoso.

4. Otorga visibilidad y control completos: Proporciona un dominio total sobre la seguridad y el rendimiento de su entorno digital.

Defensa de Nueva Generación con CiberComplet Plus

CiberSteps está impulsado por CiberComplet Plus, nuestra suite de ciberseguridad de nueva generación. Incorpora EDR (Endpoint Detection and Response), Machine Learning y Threat Intelligence para una visibilidad profunda que permite cazar, investigar y responder a incidentes que eluden las defensas tradicionales.

Solución Integral CiberControl

Esta solución revolucionaria en el sector de la ciberseguridad incluye análisis y gestión de toda su infraestructura TI. Además incorpora una plataforma integral de Monitorización y Gestión Remota (RMM) con certificación SOC 2 Tipo 1 y SOC 2 Tipo 2. Su técnico dedicado la utilizará para automatizar la gestión de parches, supervisar el rendimiento de sus sistemas y optimizar toda su infraestructura de TI de forma proactiva.

La Garantía CiberSteps

Nuestra confianza en esta solución es absoluta. CiberSteps es el único servicio del mercado respaldado por una garantía real: si sufre un ciberataque con éxito, le reembolsamos tres veces su cuota anual.

Requisitos CiberComplet Plus:

- 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 CiberSteps:

- Licencia de la Suite CiberComplet Plus
- Servicio de Técnico Dedicado y Monitorización SOC 24/7
- Solución Integral CiberControl - Análisis y Gestión de toda su Infraestructura TI
- La Garantía CiberSteps
- Auditoría Inicial, CiberTraining y Certificado ISO 27032

Todo lo que incluye CiberSafe y además:

Características	Acción	Cómo protege
EDR (Endpoint Detection and Response)	Registra y analiza toda la actividad de los endpoints (procesos, conexiones, archivos) para una visibilidad total.	Permite detectar, investigar y responder a ataques avanzados que las defensas tradicionales no ven, ofreciendo un contexto completo del incidente.
Machine Learning	Analiza enormes volúmenes de datos para crear un modelo de comportamiento normal y detectar cualquier desviación.	Identifica ataques de día cero y amenazas desconocidas basándose en su comportamiento anómalo, no en firmas de virus.
Threat Intelligence	Integra y procesa datos de inteligencia sobre amenazas a nivel mundial en tiempo real.	Reduce el ruido de los falsos positivos y enriquece las alertas, permitiendo al SOC centrarse en las amenazas reales y verificadas.
Mitre Att&Ck®	Mapea las alertas de seguridad con las tácticas y técnicas del framework global MITRE ATT&CK®.	Proporciona un contexto estandarizado para entender cómo operan los atacantes, mejorando drásticamente la eficacia de la detección y la respuesta.
Sandbox Interactive	Detona y analiza archivos o enlaces sospechosos en un entorno virtual seguro y aislado.	Determina la peligrosidad de una amenaza sin poner en riesgo la red y permite a nuestros expertos entender su funcionamiento para fortalecer las defensas.
Antiexploit Advanced	Monitoriza y bloquea las técnicas específicas que usan los atacantes para explotar vulnerabilidades en aplicaciones legítimas (navegadores, ofimática).	Previene ataques que no utilizan malware tradicional (sin archivos), protegiendo las aplicaciones que sus empleados más utilizan.
Identificación Actividades Anómalas	Alerta sobre comportamientos que se desvían de la normalidad, como accesos a horas inusuales o escalada de privilegios.	Es el núcleo de la detección proactiva, permitiendo identificar a un intruso por sus acciones, no solo por las herramientas que utiliza.
Análisis de Evidencias Digitales	Recopila y preserva datos forenses de un endpoint tras un incidente para su posterior investigación.	Proporciona la información necesaria para entender la cronología y el alcance de un ataque, fundamental para la remediación y los informes post-incidente.
Indagaciones en Línea (Threat Hunting)	Permite a los analistas del SOC lanzar consultas en tiempo real a todos los endpoints para buscar indicadores de compromiso (IoC).	Acelera drásticamente las investigaciones de seguridad, permitiendo buscar y verificar la presencia de una amenaza específica en toda la red en minutos.
Control de Dispositivos Externos	Gestiona y restringe el uso de dispositivos de almacenamiento externos como memorias USB y discos duros.	Bloquea una de las vías de entrada de malware más comunes y previene la fuga no autorizada de información corporativa.
Risk Analysis	Escanea los endpoints en busca de vulnerabilidades, configuraciones de seguridad incorrectas y software obsoleto.	Permite a su técnico asignado corregir proactivamente las brechas de seguridad antes de que puedan ser explotadas por los atacantes.

Requisitos CiberComplet Plus:

- 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 CiberSteps:

- Licencia de la Suite CiberComplet Plus
- Servicio de Técnico Dedicado y Monitorización SOC 24/7
- Solución Integral CiberControl - Análisis y Gestión de toda su Infraestructura TI
- La Garantía CiberSteps
- Auditoría Inicial, CiberTraining y Certificado ISO 27032

Todo lo que incluye CiberSafe y además:

Características	Acción	Cómo protege
Alerta Programas Inactivos	Identifica software instalado en los equipos que no ha sido utilizado durante un período prolongado.	Reduce la superficie de ataque al facilitar la desinstalación de programas obsoletos que pueden contener vulnerabilidades sin parches.
Lista Negra	Impide la ejecución de aplicaciones o el acceso a dominios y direcciones IP que están en una lista de amenazas conocidas.	Proporciona una capa de bloqueo fundamental y rápida contra malware y sitios peligrosos ya identificados por la comunidad de seguridad global.
CiberControl (Gestión Automatizada de Parches)	Identifica y despliega automáticamente las actualizaciones de seguridad que faltan en sus sistemas operativos y aplicaciones.	Reduce drásticamente la superficie de ataque al eliminar las vulnerabilidades conocidas que los delincuentes buscan explotar.
CiberControl (Monitorización y Alertas de Rendimiento)	Supervisa en tiempo real el estado de servidores, equipos y redes, generando alertas proactivas sobre posibles fallos o degradación del servicio.	Previene la inactividad no planificada y optimiza el rendimiento de su infraestructura, garantizando la continuidad y productividad del negocio.
Garantía CiberSteps	Reembolsa tres veces la cuota anual si el cliente sufre un ciberataque exitoso.	Elimina por completo el riesgo financiero de la inversión en ciberseguridad, demostrando nuestra confianza inquebrantable en la protección que ofrecemos.

General Protec

www.generalprotec.com/cibersteps/

ISO 27032