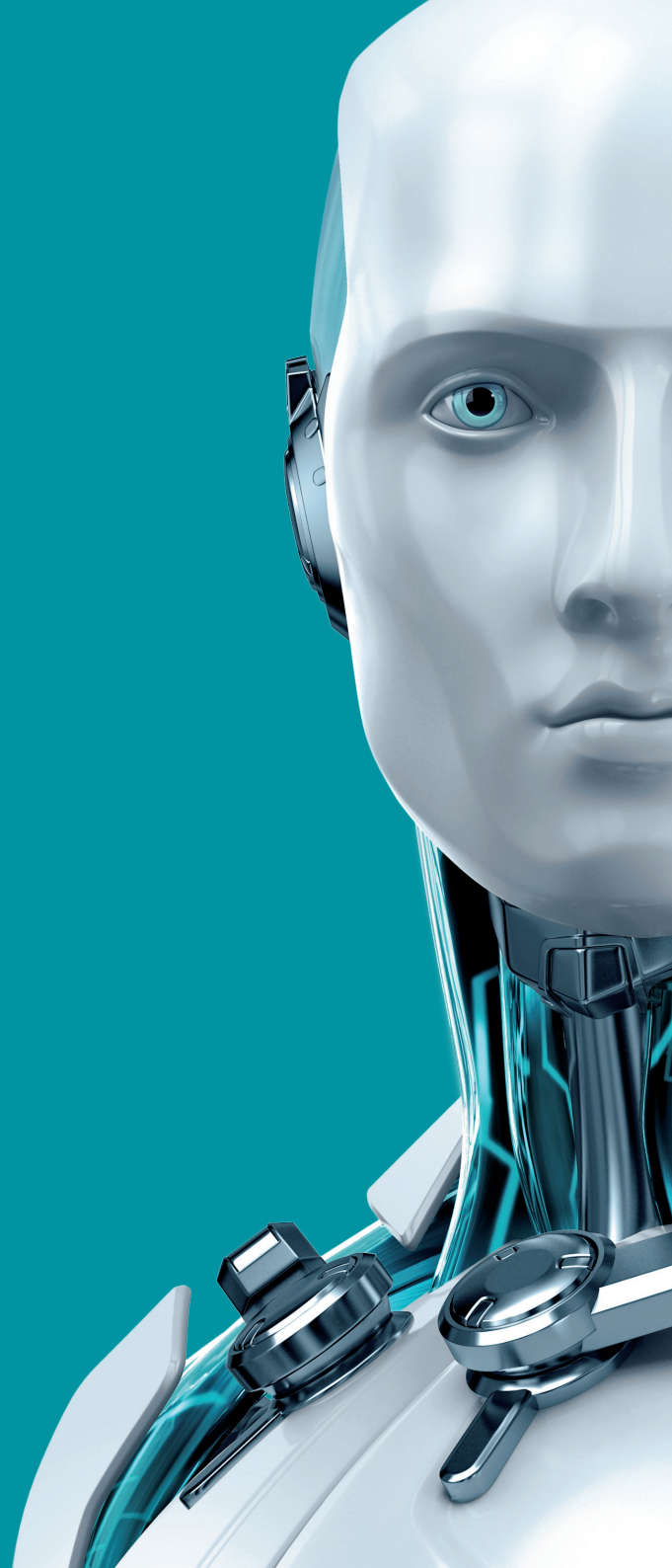
safetica

# Prevención de fugas de información

EMPRESA

ESET ALIANZA TECNOLÓGICA



El producto de seguridad Safetica ofrece una solución completa para la prevención de fugas de información (DLP). Protege a las empresas frente a una amplia gama de amenazas de seguridad con un origen común: el factor humano.

Safetica protege a las empresas contra fugas de información planificadas o accidentales, acciones internas maliciosas, problemas de productividad, los peligros que comporta la política BYOD (trae tu propio dispositivo) y mucho más.

La filosofía de seguridad de Safetica está basada en tres pilares: es completa, flexible y fácil de usar. Proporciona una solución completa para la prevención de fugas de información a nivel corporativo, enviando a los administradores informes completos de la actividad y aplicando las políticas de seguridad de la empresa en las actividades de los usuarios.

Además, cuenta con una gran ventaja: ofrecer este conjunto de herramientas de seguridad en un solo programa (en el caso de otros fabricantes se requieren diversas soluciones de seguridad).

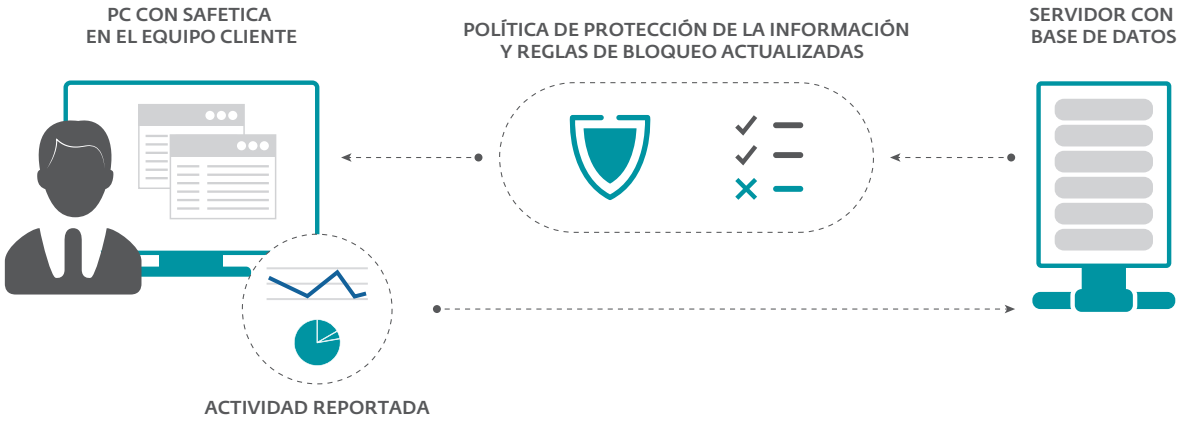


# CARACTERÍSTICAS MÁS IMPORTANTES

| | |
|---|---|
| **Solución DLP completa** | Protege los canales más importantes de fugas de información. Safetica proporciona prevención para fugas de información (DLP) en equipos de la red con estas funcionalidades. |
| **Amortización rápida** | Gracias a la flexibilidad en su configuración y con el tiempo de instalación más rápido para este tipo de productos, Safetica asegura una recuperación de la inversión en un periodo corto de tiempo. |
| **Muy difícil de alterar** | Protección robusta, incluso cuando protege a usuarios con permisos de administrador. |
| **Cubre todas las funciones contra la fuga de información** | Safetica protege la información para impedir la impresión de la pantalla, el robo mediante el portapapeles, la impresión virtual, las transformaciones de archivos y las funciones de compresión y cifrado. |
| **Enfoque escéptico** | La protección de información Safetica no está limitada por protocolos o aplicaciones individuales. |
| **Políticas de información claramente definidas** | Con Zonas Seguras. Los administradores solo tienen que especificar las rutas con información confidencial y, por tanto, no puede ser extraída. |
| **Control del tiempo exacto** | Cuando un programa está abierto no significa que esté siendo usado activamente. Los informes de actividad de Safetica muestran el tiempo real que los usuarios estuvieron activos en las páginas web visitadas o en las aplicaciones. |
| **Evaluación y alertas automáticas** | Safetica recopila los detalles registrados más importantes y envía un informe resumen a los destinatarios asignados. También están disponibles los detalles completos si los necesitas. |

# Cómo funciona

Los usuarios trabajan con información crítica de la empresa, acceden a Internet, leen correos electrónicos, envían documentos a la impresora y conectan sus dispositivos portátiles. Safetica instala un agente (Safetica Endpoint Client) en los equipos deseados y mantiene una conexión regular con ellos a través del servidor (Safetica Management Service). Este servidor construye una base de datos con la actividad de este puesto de trabajo y distribuye nuevas políticas y regulaciones para proteger la información en cada equipo.



# CARACTERÍSTICAS PRINCIPALES

| | |
|---|---|
| **Prevención completa de fugas de información** | Safetica protege todos los canales de fuga de información y es muy fácil de instalar y poner en funcionamiento. Consulta la "Cobertura de eventos de los equipos" para más información sobre la cobertura exhaustiva de Safetica. |
| **Perfiles de tendencias y productividad** | Avisa a los administradores de la empresa en caso de cambios repentinos en el rendimiento del empleado y muestra los cambios de productividad por departamento en una gráfica temporal. Estos cambios son indicaciones de posibles riesgos de seguridad. |
| **Informe de actividad** | Descubre los riesgos de seguridad en muchos frentes revisando todas las actividades de los usuarios en busca de signos de un posible peligro, incluso antes de la transferencia misma de la información. |
| **Prevención de fugas por correo electrónico** | Garantiza que la información protegida no se envía a la cuenta de correo equivocada. Registra dónde se han enviado los archivos con información sensible y almacena esta información para futuros informes. |
| **Control de aplicaciones con reglas de tiempo** | Permite un paquete seleccionado de aplicaciones relacionadas con el trabajo y bloquea otras para conseguir un entorno más seguro. Puede establecerse que las aplicaciones estén disponibles solo durante un período determinado de tiempo. |
| **Filtro web** | Permite aplicar fácilmente las Políticas de uso aceptable en la empresa (AUP, en inglés) con categorías seleccionadas cuidadosamente y filtro de palabras clave. |
| **Control de impresión** | Limita qué puede ser impreso y por quién con cuotas para usuarios y departamentos. |
| **Control de dispositivos** | Evita que los empleados puedan conectar dispositivos no autorizados en el trabajo. Los puertos comunes pueden activarse para ciertos dispositivos o bloquearse para todos. |
| **Administración del cifrado** | Safetica ofrece cifrado total del disco o cifrar particiones enteras y crear unidades virtuales locales o de red para almacenar los archivos con seguridad. Además de los métodos de contraseña y clave de acceso, Safetica ofrece la función "Traveller disk" y una característica de "Cifrar cuando se envía una copia" para la información que sale de la zona segura. |
| **Modo informativo y de pruebas** | Ayuda a las empresas a integrar progresivamente la protección de información habilitando los análisis para todas las situaciones posibles sin detener los procesos en la empresa. |
| **Clasificación de información en tránsito** | Protege la nueva información inmediatamente después de crear o recibir un archivo clasificado. |
| **Consola de administración unificada** | La consola de administración Safetica permite la gestión y creación de informes completos de seguridad, integra toda la protección de información de la empresa y las políticas de informes y bloqueo. |
| **Inspección SSL/HTTPS** | Revisa y protege las líneas de comunicación securizadas incluyendo las páginas web que utilizan el protocolo HTTPS, las aplicaciones IM con conexiones seguras y las transmisiones seguras por correo electrónico. |
| **Coste total mínimo de posesión (TCO)** | Evita a los usuarios de la necesidad de adquirir aplicaciones de seguridad adicionales. Los agentes del equipo instalados en Safetica también proporcionan características de Prevención de fugas de información para las redes de la empresa. |
| **Uso flexible** | Safetica protege todas las aplicaciones, el protocolo de mensajería instantánea o el servicio de webmail gracias a su uso universal, único en el sector. |

# ALIANZA TECNOLÓGICA

El objetivo de la alianza tecnológica de ESET es mejorar la protección de las empresas mediante una gama de soluciones complementarias de seguridad informática. Protegemos a nuestros clientes en el entorno de la seguridad informática, que está en constante evolución, mediante la combinación de nuestra eficaz y fiable tecnología con otros productos que son los mejores en su campo.


## Cobertura de eventos en los equipos

### Informes y bloqueo de actividad

- Operaciones de todos los archivos.
- Tendencias a largo plazo, fluctuaciones de actividad a corto plazo.
- Páginas web (compatible con todos los navegadores, incluyendo el tráfico HTTPS). Tiempo activo e inactivo.
- Correo electrónico y webmail (prácticamente todos los proveedores).
- Palabras clave buscadas (compatible con la mayoría de buscadores y con Windows Search).
- Mensajería instantánea (independiente de las aplicaciones. Todos los protocolos).
- Uso de la aplicación mostrando tanto el tiempo activo como inactivo.
- Impresoras virtuales, locales y en red.
- Actividad de la pantalla (captura inteligente).

### Prevención de fugas de información

- Todos los discos duros, USB, FireWire, tarjetas SD/MMC/CF, unidades SCSI.
- Transferencia de archivos en red (no protegidos, protegidos).
- Correo electrónico (protocolos SMTP, POP, IMAP, Microsoft Outlook/MAPI).
- SSL/HTTPS (todos los navegadores y aplicaciones con administración de certificados estándar).
- Copiar/Pegar, portapapeles, arrastrar y soltar.
- Impresoras virtuales, locales y en red.

# Casos de uso

| | |
|---|---|
| **Protección para la información importante de la empresa** | Una vez establecidas las zonas seguras para toda la información protegida, Safetica comprueba de forma silenciosa cada interacción con estos archivos y, en caso de una operación no autorizada, la bloquea o realiza otra acción programada. Estas acciones definidas por la empresa pueden incluir informar de cada evento al administrador de la seguridad, cifrar la información y ofrecer otra ubicación segura para ella. La información está protegida incluso fuera de la oficina, en portátiles y unidades extraíbles. |
| **Administración de dispositivos extraíbles** | Safetica proporciona a los administradores el control final sobre quién conecta y qué se conecta en los equipos de la empresa, eliminando así otro canal de fuga de información y disminuyendo drásticamente el número de intervenciones necesarias. |
| **Cumplimiento de políticas** | Con Safetica Endpoint Client presente en los equipos de la empresa y la administración de políticas activada en la consola de administración de Safetica, puedes cumplir las regulaciones que rigen el movimiento y el uso de información confidencial. |
| **Cifrado de información** | Safetica ofrece "Cifrado total del disco". Puede supervisar un sistema de almacenamiento de archivos cifrado, administrar los USB conectados y evitar que la información sea almacenada en ubicaciones no seguras. |
| **Productivity Control** | Incluso sin utilizar directamente la interfaz de usuario de la consola de administración de Safetica, los administradores pueden recibir informes periódicos sobre determinados usuarios o grupos. |

# Arquitectura


1. Un agente se encarga de guardar las acciones y aplicar las políticas en el equipo (con opción de ocultarlo al usuario).
2. La información se transfiere automáticamente de los ordenadores de la red al servidor. La información de los portátiles se sincroniza en el momento en que éstos se conectan a la red.
3. Toda la información puede consultarse desde la aplicación de administración y también se pueden modificar los ajustes.
4. Safetica permite controlar múltiples sucursales desde una única consola de administración central.

# Requisitos del sistema

### Safetica Endpoint client (agente)

- Procesador dual-core de 2,4 GHz de 32 bits (x86) o 64 bits (x64)
- 2 GB de memoria RAM
- 2 GB de espacio libre en disco
- Instalación en el equipo cliente
- MS Windows XP SP3, Vista, 7, 8, 8.1 y 10 de 32 bits y 64 bits
- Paquete de instalación MSI

### Safetica Management Service (servidor)

- 2 GB de memoria RAM
- 10 GB de espacio libre en disco
- Instalación en un servidor de aplicaciones o en un servidor dedicado (puede ser virtualizado)
- Más servidores para una mejor disponibilidad del balanceo de carga
- Compatible con Active Directory
- MS Windows Server 2008, 2008 R2 y 2012 R2, de 32 bits y 64 bits
- Requiere conexión al servidor con MS SQL 2008 o superior

### MS SQL (servidor)

- Procesador de 1 GHz de 32 bits (x86) o 64 bits (x64)
- 4 GB o más de memoria RAM (importante)
- 200 GB de espacio libre en disco (óptimo 500 GB o más. Más detalles en: www.safetica.com)
- Servidor compartido o dedicado MS Windows Server 2003 SP2, 2008 y 2008 R2, de 32 bits y 64 bits