

Aranda Security Compliance

Solución de cumplimiento regulatorio
para seguridad de la información



Aranda Security Compliance (ASEC) es una solución integral que audita el cumplimiento de software de seguridad y sus configuraciones, además de detectar de manera proactiva vulnerabilidades en el software, reforzando significativamente la postura de seguridad de su organización.

Desafíos de ciberseguridad en el entorno de TI empresarial

A medida que las organizaciones han adoptado acciones para facilitar el desempeño de sus colaboradores en cualquier lugar (como el trabajo remoto, uso de dispositivos personales y soluciones basadas en la nube), los riesgos de seguridad de la información corporativa han aumentado exponencialmente y a consecuencia de ello, los ciberataques se han convertido en una preocupación constante de las áreas de TI. En el año 2022, ocurrieron más de **360 mil millones de intentos de ataques informáticos** a empresas de Latino América, nueve (9) veces más con respecto al año 2020¹.

Fortalecer la **postura de seguridad** de las empresas conlleva una serie de desafíos a ser tomados en cuenta si se desea mantener competitividad en el mercado y evitar la exposición a penalidades, pérdida de reputación y fuga de clientes, como los siguientes:

- ¿Qué tan **segura** es mi empresa?
- ¿Estamos adoptando y poniendo en práctica la **estrategia de ciberseguridad** correcta?
- ¿Qué tan eficientes son nuestros **controles de seguridad**?
- ¿Cómo **demostramos cumplimiento** con estándares o prácticas de seguridad informática requeridos en la organización? (ej. ISO 27001, CIS Controls)

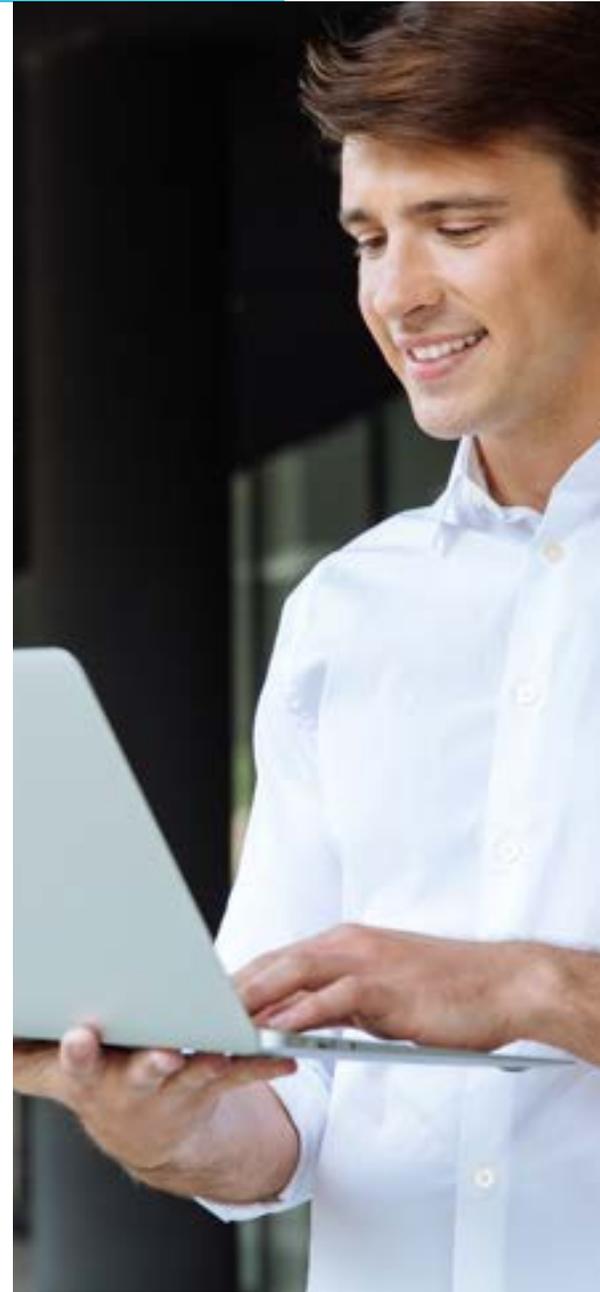
¹ Informe Semestral FortiGuard Labs, 2022

- ¿Cómo poner en práctica tareas eficaces de cumplimiento de seguridad informática en la organización, cuando tenemos **múltiples tecnologías de seguridad** (ej. Firewall, Antimalware, Data Loss Prevention) y poco personal especializado?

Aranda Security Compliance: La solución para automatizar la gestión de cumplimiento de seguridad de su organización

Aranda Security Compliance (ASEC) permite a las organizaciones demostrar cumplimiento con marcos regulatorios como HIPAA, GDPR y PCI DSS al **entregar visibilidad de sus dispositivos** respecto a protección de seguridad, reduciendo riesgos inherentes de operación y maximizando el valor de su inversión en TI al reducir las brechas de seguridad.

A través de ASEC, podrá identificar de manera rápida e intuitiva las **vulnerabilidades** presentes en el software de sus dispositivos y evaluar su **estado de cumplimiento de seguridad**. Además, le permitirá ejecutar **tareas de remediación** en aquellos equipos que no cumplan con las políticas definidas en su empresa, **reduciendo así la exposición** a brechas de seguridad y **habilitando un entorno de trabajo seguro**, sin importar la ubicación de sus usuarios o la diversidad de fabricantes de soluciones de seguridad utilizados en su organización.



Qué preguntas podemos responder a través de ASEC?

- ¿Cuáles equipos (tanto corporativos como de uso personal) **no cumplen con las políticas de seguridad** definidas en la empresa?
- ¿Existen aplicaciones de seguridad instaladas con **versiones obsoletas/no autorizadas** y propensas a vulnerabilidades?

- ¿Qué vulnerabilidades críticas se encuentra en el **software instalado**, dentro de mi parque de dispositivos, que podrían ser explotadas por atacantes? ¿qué puedo hacer para mitigarlas antes de que se conviertan en una **amenaza para la seguridad** de la organización?
- ¿Los **usuarios están desactivando** por su cuenta servicios de seguridad (como el firewall, el antimalware) a pesar de la definición establecida en la organización?
- ¿Se ha **realizado respaldo** recientemente en los equipos, con la solución de respaldos usada en la empresa?
- ¿Cómo **activar de forma masiva** en los equipos afectados, las **soluciones de seguridad** instaladas? (ej. iniciar el servicio de Firewall, activar protección en tiempo real)
- ¿Cómo **disminuir costos** por la recuperación de dispositivos afectados por ciberataques?
- ¿Cómo **demostrar evidencia de cumplimiento** ante el regulador (local, sectorial, internacional) de las políticas de seguridad de la organización?

Maximizando su inversión en seguridad informática

A diferencia de otras soluciones de gestión TI que solo se limitan a verificar la instalación del software de seguridad, ASEC no solo asegura que el software esté correctamente instalado y funcionando, sino que también identifica las vulnerabilidades presentes en el software, permitiendo a las organizaciones tomar medidas proactivas para mitigarlas.

Dentro de sus capacidades de Compliance, ASEC ofrece una evaluación rápida de aspectos clave, como:

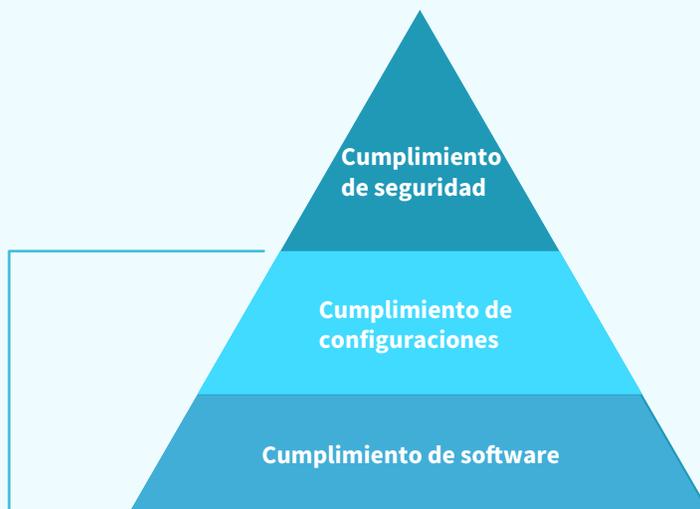
- Estado de ejecución
- Protección en tiempo real (para aplicaciones antimalware)
- Estado de respaldos (para aplicaciones de respaldo y recuperación)
- Protección contra phishing
- Estado de encriptación de disco
- Estado de encriptación de datos



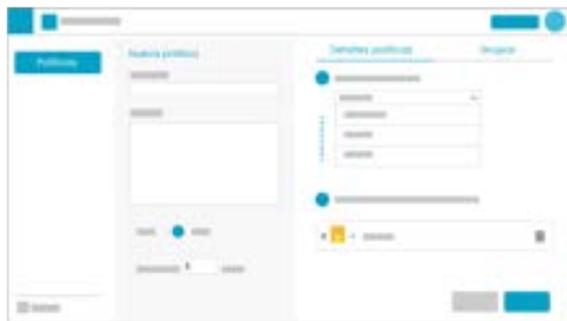
A partir de la identificación del estado de los dispositivos, Ud. podrá remediar rápidamente los equipos que no cumplen con la política de seguridad, iniciando de forma desatendida acciones automáticas como la activación de las soluciones de seguridad (ej. iniciar el firewall) y la activación de la protección en tiempo real (para aplicaciones de malware), entre otras.

“La base para el cumplimiento de seguridad en su organización”

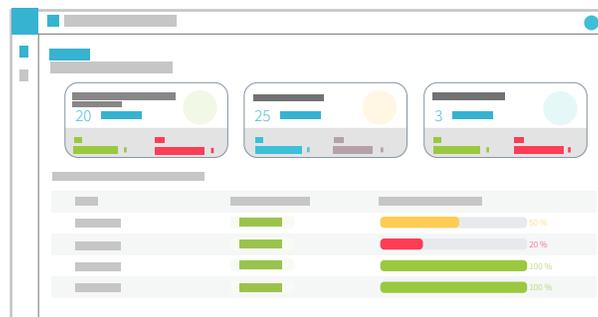
ASEC



Solución rápida y efectiva para cumplimiento de seguridad



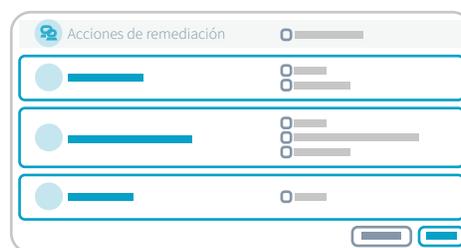
Defina las políticas de cumplimiento



Identifica rápidamente el nivel de cumplimiento



Selecciona los equipos fuera de cumplimiento



Aplica las acciones de remediación correspondientes

Características principales

- ✓ Solución **100% Cloud**
- ✓ Implementación **ágil y rápida.**
- ✓ Compatibilidad con los **fabricantes más reconocidos** en soluciones de seguridad (Acronis, Avast, AVG, CheckPoint, ESET, Fortinet, Kaspersky, McAfee, Microsoft, Symantec, TrendMicro).
- ✓ Soporta más de 10 tipos de soluciones de seguridad, desde el primer día: Antimalware, Antiphishing, Antivirus, Data Loss Prevention (DLP), Encriptación, Firewall, Respaldo, VPN, entre otras.
- ✓ **Dashboard** para estado general de cumplimiento
- ✓ **Remediación inmediata** para equipos fuera de cumplimiento.
- ✓ Compatibilidad con sistemas operativos Windows, MacOS (*) y Linux (*)

Beneficios de ASEC para su organización

- **Mejora la toma de decisiones** de seguridad informática, al contar con una solución centralizada que informa en tiempo real del estado de cumplimiento de sus políticas de seguridad.
- **Minimiza tiempos muertos** por intervenciones de seguridad en los equipos debido a configuraciones de seguridad incompletas/obsoletas.
- **Fortalece la postura de seguridad** de su organización, gracias a la visibilidad de los activos tecnológicos y su superficie de ataque.
- **Facilita el cumplimiento regulatorio** de su organización, al demostrar evidencia requerida para cumplir con normativas como ISO 27001, Controles CIS, HIPAA, PCI DSS, entre otros.
- **Reduce el error humano** por intervenciones manuales en los equipos de su organización.
- La **detección proactiva de vulnerabilidades** en el software reduce significativamente el riesgo de explotación de fallas, fortaleciendo la protección contra ataques cibernéticos y mejorando la seguridad general de su entorno TI.

*Compatibilidad con MacOS y Linux a partir de Q1 2024.

Entorno TI más seguro con Aranda Software

Complemente las capacidades de Aranda Security Compliance con las siguientes soluciones de nuestro portafolio que juntas, contribuyen a un entorno TI más productivo y preparado para responder ante amenazas de seguridad:

- **Software Delivery:** Reduzca los costos operativos de soporte TI al desplegar de forma centralizada paquetes de aplicaciones de software que deben estar instaladas en los equipos.
- **Patch Management:** Elimine brechas de seguridad por aplicaciones no parchadas (tanto de Microsoft como de terceros -ej. Adobe, Cisco, Google, Oracle, Zoom) al identificar y desplegar automáticamente los parches faltantes en los equipos.

