

**Cumplimiento de SOX con
Aranda 360 ENDPOINT SECURITY**



Enero 2009

TABLA DE CONTENIDO

INTRODUCCIÓN	3
De qué se trata la Ley SOX	3
Nuevas tecnologías y las prácticas comerciales	4
Utilizando Aranda 360 ENDPOINT SECURITY para cubrir las brechas	6
CORRESPONDENCIA CON SOX.....	10
CONCLUSIONES	17

INTRODUCCIÓN

De qué se trata la Ley SOX

La Ley Sarbanes-Oxley es una ley federal de los Estados Unidos que ha generado mucha controversia, ya que esta va en respuesta a los escándalos financieros de algunas grandes corporaciones, entre los que se incluyen los casos que afectaron a empresas tales como Enron, Tyco International, WorldCom y Peregrine Systems.

Esta ley fue aprobada por amplia mayoría, tanto en el congreso como el senado. La legislación abarca y establece nuevos estándares para los consejos de administración y dirección y los mecanismos contables de todas las empresas que cotizan en la bolsa de los Estados Unidos. Introduce responsabilidades penales para el consejo de administración y establece unos requerimientos por parte de la SEC (Securities and Exchanges Commission), es decir, la comisión reguladora del mercado de valores de Estados Unidos. Los partidarios de esta ley afirman que la legislación era necesaria y útil, mientras los críticos creen que causará más daño económico del que previene.

La primera y más importante parte de la ley establece una nueva agencia: La Junta de Supervisión Contable de Entidades Públicas, es decir, una compañía reguladora que se encarga de revisar, regular, inspeccionar y disciplinar a las auditoras. La ley también se refiere a la independencia de las auditoras, el gobierno corporativo y la transparencia financiera. Se considera uno de los cambios más significativos en la legislación empresarial, desde el “New Deal” de 1930.

Las empresas no lo pueden negar: aunque polémico, el cumplimiento de la ley Sarbanes-Oxley (SOX) se encuentra en un elevado nivel dentro de la lista de iniciativas de seguridad para cualquier entidad pública. SOX es un proyecto en curso que exige atención continua y que muchos departamentos responsables de TI ya se encuentran atendiendo. Debido a que las regulaciones de SOX exigen que los altos ejecutivos den testimonio de la integridad de sus sistemas internos, este esfuerzo continúa atrayendo el escrutinio de los más altos niveles de administración dentro de las empresas públicas. Cualquier esperanza de que esta ley se disuelva se ha desvanecido.

“La última apelación contra la ley SOX fue interpuesta por Free Enterprise Fund., quien argumentaba que la Junta de Supervisión Contable de Entidades Públicas era inconstitucional y violaba la separación de poderes en conjunto con otras tres oficinas de entidades federales. En marzo de 2007 la Corte del Distrito de Estados Unidos para el distrito de Columbia negó la apelación.”

La ley no define específicamente la forma como un departamento de TI debe aplicar los controles de seguridad. Esto significa que la orientación de la Junta de Supervisión Contable de Entidades Públicas dicta que cualquier marco de seguridad utilizado, debe cumplir las recomendaciones de la Comisión de Organizaciones Patrocinadoras (COSO). El marco de trabajo más utilizado es el de Objetivos de Control para la Información y Tecnología (COBIT). La mayoría de las empresas ya han completado el esfuerzo inicial de cumplir con SOX. Sin embargo, este esfuerzo debe extenderse hasta garantizar que no se generen nuevos riesgos al implementar nuevas tecnologías.

Nuevas tecnologías y las prácticas comerciales

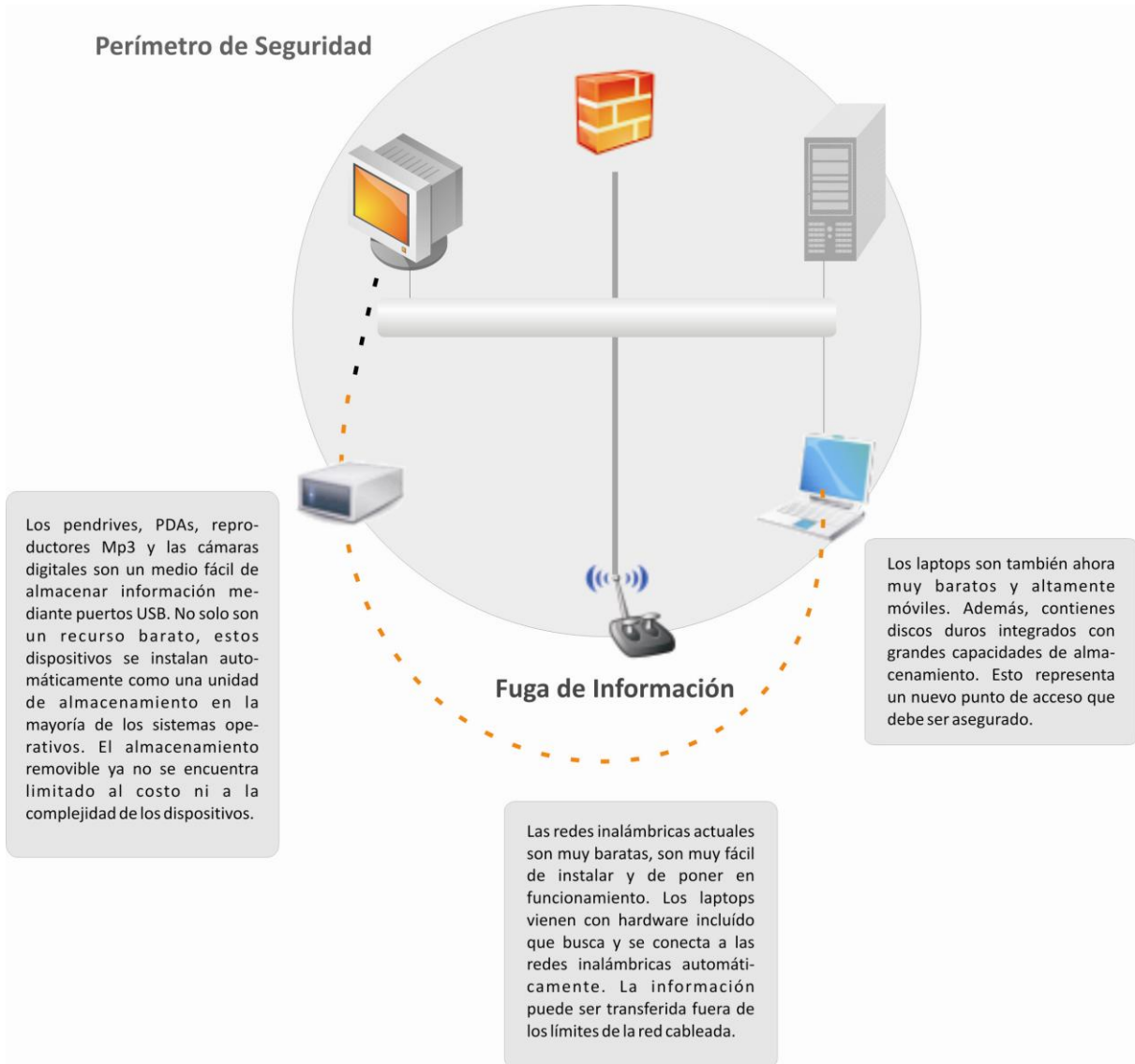
La clave al requerimiento de SOX es garantizar la integridad de cualquier sistema de TI que tenga acceso a información financiera.

El requerimiento no es nuevo - pero SOX exige la rendición de cuentas e introduce la obligación de ejecución del cumplimiento. No es de extrañar que la mayoría de las soluciones traten de resolver el problema con métodos clásicos.

El enfoque clásico para asegurar la información electrónica implica la definición de un perímetro de seguridad que separe los entornos. Se limita el acceso a la información sensible desde sistemas localizados en el interior del perímetro. El acceso a estos sistemas también se controla internamente. El acceso desde afuera sólo es controlado a través de puntos de acceso específicos, por ejemplo, desde un firewall o cortafuegos. Esta estrategia supone que el perímetro impide cualquier otro tipo de transferencias de información y el firewall es el único que permite el acceso.

Este modelo funcionó muy bien, pero sólo en el mundo de las redes de cableado y de los dispositivos fijos de almacenamiento. En ese mundo, las estaciones de trabajo estaban atadas por su conexión de red, por lo que no podían ser transportadas fácilmente. Las limitaciones físicas de los equipos reforzaban el control de acceso. Además, la mayoría de estas estaciones de trabajo no contenían almacenamiento extraíble, de modo tal que el acceso a la información era físicamente más restringido. El firewall corporativo representaba la única forma de transferir información entre estos puntos finales. Los profesionales de seguridad consideraban que sus principales preocupaciones eran velar porque el firewall se mantuviera en buenas condiciones y que detuviera los ataques externos.

Sin embargo, varias tecnologías nuevas han surgido para cambiar este contexto. Las infraestructuras actuales de TI de las compañías hacen muy difícil que la base de su seguridad se implemente en un único punto de control de acceso.



Todas estas nuevas tecnologías crean brechas de seguridad dentro de la infraestructura tradicional de seguridad, por lo que la información puede ahora fluir desde y hacia la red corporativa sin protección o seguridad.

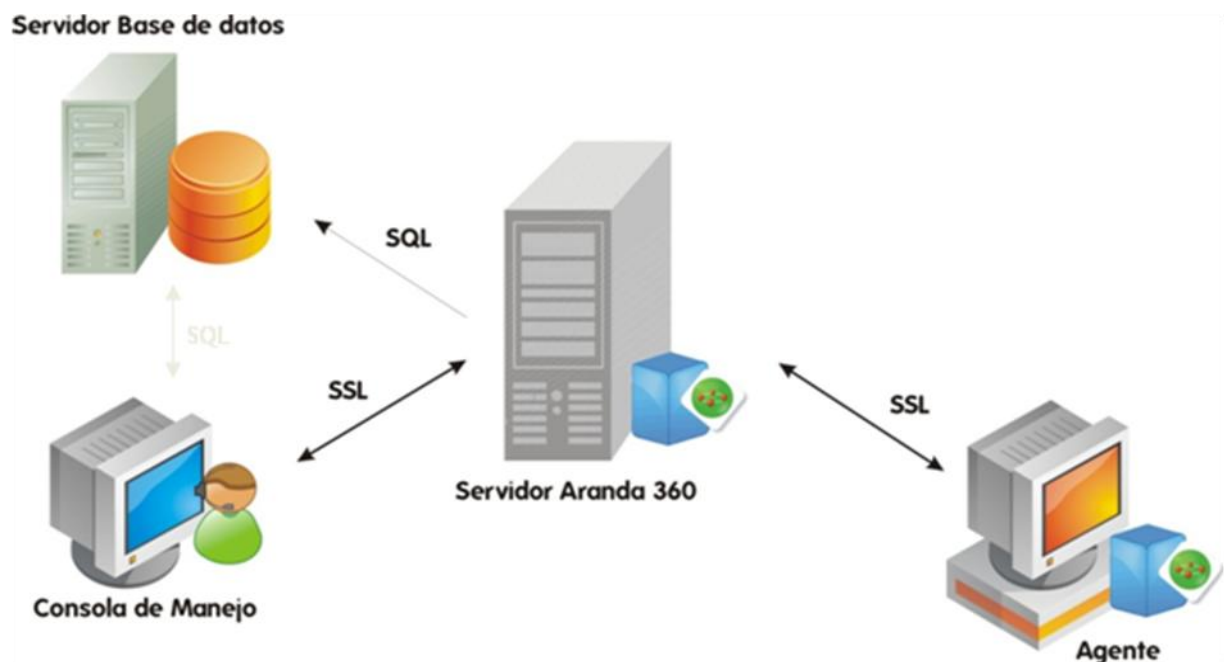
Utilizando Aranda 360 ENDPOINT SECURITY para cubrir las brechas

Aranda 360 proporciona un completo conjunto de módulos de control de acceso que limitan estos nuevos riesgos. Estos productos ofrecen un alto grado de control sobre los mecanismos de acceso en el punto final: Pueden impedir la transferencia no autorizada o la "fuga de datos". Los productos tienen capacidades clave para abordar estos problemas en concreto y que ayudan al cumplimiento de los requerimientos de SOX.

COBIT tiene una estructura específica de cuatro dominios para seleccionar e implementar controles de seguridad:

1. Planificar y Organizar
2. Adquirir y Aplicar
3. Entregar y Soportar
4. Monitorear y Evaluar

Aranda 360 ENDPOINT SECURITY proporciona características que abordan la problemática de fugas de datos en todos los cuatro dominios de COBIT.



Planificar y organizar

Uno de los primeros requisitos de COBIT es realizar una evaluación de la infraestructura existente para determinar sus fortalezas y debilidades. **Aranda 360** permite al administrador de la solución recopilar información de cada punto final y entregar un reporte completo de los dispositivos, puertos y conexiones que se encuentran en uso. A medida que se desarrollan planes, las funciones deben ser definidas y mantenidas por la organización. Esto es especialmente cierto para las tareas administrativas. Una vez establecido, el acceso a la información debe estar asociado a cada uno de los roles. Aranda 360 permite definir y aplicar políticas de seguridad y de acceso a los archivos de acuerdo a esos roles. Las reglas de acceso a la información se pueden asociar fácilmente con estas políticas y distribuir las a todo el sistema. Aranda 360 también contiene una función de administración que tiene el control exclusivo de la creación y distribución de la política.

COBIT obliga a que un departamento de TI minimice el costo de la reducción de riesgos. Aun así, la reducción del riesgo debe incluir controles preventivos, correctivos y de detección. Aranda 360 ENDPOINT SECURITY se integra fácilmente con la infraestructura de seguridad existente, garantiza un bajo costo y las mínimas interrupciones en el negocio. Aranda 360 integra las capacidades de administración para asegurar que el sistema se pueda mantener eficientemente. Esto incluye la modificación de los permisos de acceso de usuario y la identificación de cualquier intento de violación a la política de acceso.

Adquirir y aplicar

Una vez que el plan ha sido elaborado, el siguiente paso es la realización a través de la adquisición y aplicación de la tecnología. Cualquier tecnología elegida debe estar en capacidad de satisfacer las exigencias del plan. Aranda 360 ENDPOINT SECURITY contiene un completo conjunto de características incluyendo:

- Controles preventivos, que restringen el acceso no autorizado a la información en el punto final.
- Controles de detección, que proporcionan capacidades de auditoría de acceso a la información y a las aplicaciones.
- Controles correctivos, los cuales generan alarmas y bloquean dispositivos y aplicaciones tipo malware como *keyloggers* instalados en el punto final.

Utilizando los resultados de Aranda 360, es posible crear desde la Consola de Administración un conjunto de políticas para todos los puntos finales. Un administrador del sistema puede implementar una política para cada uno de los dispositivos descubiertos en la auditoría. Esto asegurará fundamentalmente el flujo de información en el punto final.

Entregar y Soportar

El dominio de Entrega y Soporte es muy dependiente de las características de seguridad de los productos que un cliente elige. Este se ocupa principalmente de cómo las soluciones de seguridad seleccionadas se alinean con los objetivos de la empresa. Lo que sigue es un resumen de los ámbitos en los que Aranda 360 proporciona soporte en el cumplimiento.

Confidencialidad, integridad y disponibilidad de la información sensible: En primer lugar, las cuentas de usuario se deben estar establecidas para administrar los permisos de acceso. Aranda 360 puede utilizar cuentas o grupos de usuario explícitamente definidos en sistemas de gestión existentes, por ejemplo, Active Directory para aplicación de las políticas de seguridad. Los permisos de acceso se pueden definir para usuarios o grupos individuales y que pueden limitar tanto el acceso a la información como las transferencias de datos a dispositivos externos - incluidos los de almacenamiento extraíble y conexiones inalámbricas tanto para uso dentro del sitio como fuera de este.

Monitoreo de uso de la información: Aranda 360 ENDPOINT SECURITY permite obtener en cualquier momento un reporte completo de todos los dispositivos extraíbles no autorizados utilizados en el punto final. Después de que las políticas de acceso han sido desplegadas, Aranda 360 monitorea el flujo de la información. Cualquier violación de acceso se registra en el *log* de auditoría. Utilizando la consola de administración es posible definir condiciones de generación de alertas y asociarlas a las políticas. Opcionalmente, es posible enviar las alertas a un administrador designado para tomar medidas correctivas. Además, los *logs* proporcionan una historia completa de todos los eventos, de tal forma que una línea de tiempo puede ser fácilmente reconstruida en una fecha posterior.

Proteger contra las amenazas: Como se mencionó anteriormente, la tecnología móvil plantea un nuevo desafío. El robo o la pérdida de los dispositivos de almacenamiento, tanto internos como externos, es una preocupación constante. Aranda 360 mitiga esta amenaza asegurando la información en un formato encriptado y su confidencialidad se mantendrá si esta amenaza se materializa. La arquitectura de Aranda 360 también permite crear roles de administración para controlar el acceso a las configuraciones. Lo que es más, una vez creadas las políticas y las configuraciones, estas se envían utilizando canales seguros de comunicación (SSL).

Monitorear y evaluar

El cuarto dominio se centra en la medición continua del desempeño de la infraestructura de TI implementada. Aranda 360 recopila una amplia variedad de información de registro y de auditoría:

- **Log del Sistema** - Registra actividades de ejecución de aplicaciones, uso de puertos, acceso al registro del sistema operativo y acceso a los archivos. Cada registro informa un evento específico.
- **Log de Dispositivo** - Registra actividad de uso de dispositivos, como la conexión de un dispositivo removible, almacenamiento de datos en discos duros externos o CD / DVD.
- **Log de la Red** - Información sobre el control y filtrado de tráfico. Conexiones entrantes y salientes desde los puntos finales, eventos del IDS.

- **Log del Agente** - Registra eventos exclusivos de la actividad del agente de seguridad como el estado, la aplicación de una configuración o de una política, la desactivación de la protección, etc.

El agente de Aranda 360 envía los registros y alertas hacia el servidor para su almacenamiento en una base de datos y monitoreo desde la consola de administración. Desde allí pueden ser consultados por un administrador en cualquier momento.

CORRESPONDENCIA CON SOX

La siguiente sección muestra una lista detallada de requerimientos de SOX (COBIT) y cómo Aranda 360 ENDPOINT SECURITY ayuda en el cumplimiento de éstos.

Sección de CobiT	Resumen del Requerimiento	Que hace Aranda 360
PO1 Definir un plan de TI estratégico		
PO 1.3 Evaluación de desempeño actual	Realizar una evaluación de la infraestructura existente que incluya el análisis de sus fortalezas y debilidades.	Aranda 360 ENDPOINT SECURITY proporciona una vista completa de los puertos, dispositivos, aplicaciones y las redes en uso por los usuarios de su organización, así como un historial de lo que se utilizó anteriormente. Al revisar este informe, los propietarios de la información pueden determinar si está autorizado el acceso a almacenamiento extraíble o a las redes inalámbricas.
PO 4 Definir los procesos, organización y relaciones de TI		
PO 4.6 Roles y responsabilidades	Las funciones y responsabilidades deben ser definidas y comunicadas en toda la organización. Una vez creadas, estas funciones deben mantenerse.	Las políticas de Aranda 360 pueden ser aplicadas o distribuidas de acuerdo al usuario o grupo de seguridad de Microsoft Active Directory. Además, los roles de administración se pueden definir desde la consola. Esto restringe el acceso a las políticas y a las funciones de identificación y autorización únicamente a los administradores de la solución.
PO 4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento	Se deben crear funciones específicas para tareas críticas que implican la gestión del riesgo para la seguridad de la información y el cumplimiento.	Aranda 360 ENDPOINT SECURITY permite el establecimiento de administradores que puedan definir e implementar políticas de control de acceso. Los usuarios finales no podrán modificar las políticas una vez que éstas hayan sido distribuidas.
PO 4.9 Propiedad de datos y de sistemas	Se deben definir propietarios de la información crítica y proveer sistemas que refuercen la clasificación de los datos.	Es posible definir políticas de encriptación que permitan establecer la propiedad de los datos de los usuarios. Se proveen mecanismos adicionales para determinar cómo los usuarios finales pueden tener acceso a datos sensibles.

PO6 Comunicar las aspiraciones y la dirección de la gerencia		
PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI	La dirección debe elaborar un marco de trabajo de control empresarial para TI a un alto nivel con costos mínimos y definir y comunicar las políticas. La reducción de riesgos debe incluir medidas preventivas, investigativas y correctivas para proteger los objetivos del negocio.	La suite de Aranda 360 ENDPOINT SECURITY se integra fácilmente en ambientes existentes con una mínima cantidad de esfuerzo de integración. Una vez implementada, la suite ofrece: <ol style="list-style-type: none"> 1. Control del punto final y protección de la información sensible. 2. Limitación a las pérdidas de datos mediante la eliminación del acceso inherente a los medios extraíbles de almacenamiento. 3. Funcionalidades de alerta para la identificación oportuna de violaciones a las políticas establecidas.
PO7 Administrar los recursos humanos de TI		
PO7.8 Cambios y terminación de trabajo	En caso de un cambio en los puestos de trabajo o de terminación de un contrato, se deben redefinir los derechos de acceso y reasignar responsabilidades con el fin de minimizar riesgos y garantizar la continuidad de la función.	Mediante las capacidades de auditoría, Aranda 360 identifica los usuarios que tienen accesos a las aplicaciones, archivos y dispositivos. Es posible modificar las políticas de uso de los recursos cuando las funciones cambian.
PO9 Evaluar y administrar los riesgos de TI		
PO9.3 Identificación de eventos	Las posibles amenazas a la infraestructura deben ser identificadas, junto con el impacto potencial.	Aranda 360 ENDPOINT SECURITY ofrece informe detallado de cada punto final: Información que muestra cada uno de los dispositivos de almacenamiento externo que han sido conectados o desconectados. El <i>log</i> de actividades reporta qué archivos han sido transferidos a los medios extraíbles o a clientes de correo y mensajería instantánea. Los administradores pueden consultar esta lista de archivos para determinar si alguno de los medios removibles utilizados por los usuarios contiene información sensible.
AI2 Adquirir y mantener software aplicativo		

<p>AI2.3 Control y auditabilidad de las aplicaciones</p>	<p>Las aplicaciones utilizadas para aplicar controles en las empresas deben contener: mecanismos de autorización, integridad de la información, control de acceso, copia de seguridad y el diseño de registros de auditoría.</p>	<p>Aranda 360 provee medidas de seguridad que se puedan incorporar en un completo conjunto de controles para la gestión del acceso a la información. Por ejemplo, la suite de Aranda 360 incluye: Prevención: Controla el acceso a los datos y a las aplicaciones en el punto final. Detección: Proporciona controles de detección, en forma de auditoría y alertas, para complementar los controles de prevención. Corrección: Aranda 360 detecta y bloquea keyloggers, spyware, rootkits y malware.</p>
<p>AI2.4 Seguridad y disponibilidad de las aplicaciones.</p>	<p>Direccionar los riesgos identificados que conllevan a derechos de acceso y protección de la información en todas las etapas.</p>	<p>La capacidad de definición de políticas en Aranda 360 permite crear controles de acceso individuales para cada dispositivo. La política define el tipo de acceso que el usuario tendrá a varios puertos y dispositivos de almacenamiento. Esto permite al administrador bloquear o impedir la transferencia de datos a través de las aplicaciones.</p>
<p>DS5 Garantizar la seguridad de los sistemas</p>		
<p>DS5.4 Administración de cuentas del usuario</p>	<p>Implementar la administración de cuentas de usuario que incluya: solicitar, establecer, expedir, modificar, suspender y cerrar las cuentas de usuario.</p>	<p>Puesto que Aranda 360 ENDPOINT SECURITY se integra con Microsoft Active Directory, las políticas de seguridad se pueden aplicar de forma dinámica a nivel de usuario o de grupo de seguridad.</p>
<p>DS5.5 Pruebas, vigilancia y monitoreo de la seguridad</p>	<p>Cualquier implementación de aplicaciones de TI debe tener una función de monitoreo y registro que proporcione la detección temprana de actividades no autorizadas.</p>	<p>La suite de Aranda 360 ENDPOINT SECURITY incluye varios tipos de registros: Sistema - Información sobre eventos correspondientes al sistema operativo, el uso de las aplicaciones y los archivos. Dispositivos - Información correspondiente a eventos relacionados con el uso de dispositivos removibles y Wi-Fi. Red - Registra los eventos sobre el uso de la red, Firewall e IDS.</p>

		<p>Agente - Información correspondiente al comportamiento del agente de seguridad en cada cliente, informa la aplicación de una política o el estado de actividad.</p>
<p>DS5.6 Definición de incidente de seguridad</p>	<p>Los incidentes de seguridad deben estar claramente definidos para garantizar que la respuesta siga el proceso de respuesta a incidentes.</p>	<p>Al definirse una política de seguridad en Aranda 360, esta incluye la opción de generar alertas o <i>logs</i> de eventos. Al detectarse un intento de violación de la política, el evento se registra en un archivo o se envía a través de correo electrónico. La configuración de las alertas se puede definir a nivel específico de la política o a nivel general por evento.</p>
<p>DS5.7 Protección de la tecnología de seguridad</p>	<p>Todas las funciones relacionadas con la seguridad deben ser resistentes a manipulaciones, de tal forma que no puedan ser sobrepasadas por cualquier acceso no autorizado.</p>	<p>La consola de administración de Aranda 360 es utilizada para crear y modificar las políticas de seguridad y se encuentra separada de los puntos finales. Una vez las políticas han sido definidas, estas se pueden distribuir a los puntos finales mediante el uso de conexiones SSL seguras.</p>
<p>DS5.10 Seguridad de la red</p>	<p>La información que fluye desde y hacia las redes debe controlarse con técnicas de seguridad y con los procesos de gestión relacionados.</p>	<p>Aranda 360 permite definir políticas que especifican cómo se puede acceder a las redes inalámbricas desde el punto final. Dos tipos de controles se encuentran disponibles:</p> <ol style="list-style-type: none"> 1- Especificar los tipos de conexión a los que se permite el acceso. 2- Determinar las redes específicas a las cuales se permite el acceso. <p>Al hacer uso de estas políticas, Aranda 360 crea un grupo de listas blancas o listas negras, con el fin de prevenir cualquier transferencia de información sobre redes inseguras o no permitidas.</p>
<p>DS5.11 Intercambio de datos sensitivos</p>	<p>Se requieren controles necesarios para garantizar la seguridad en la transferencia de información</p>	<p>Dependiendo del dispositivo removible de almacenamiento conectado, Aranda 360 puede forzar la encriptación de toda</p>

	sensible.	<p>la información almacenada en ese dispositivo. Como regla, los dispositivos removibles encriptados de la organización solo pueden conectarse en equipos protegidos por el agente de Aranda 360. Una función opcional permite o deniega el acceso a los archivos en computadores que no pertenezcan a la red corporativa.</p> <p>Para los dispositivos que no se encuentren encriptados, se pueden definir políticas de tal forma que controle el tipo de acceso a la información contenida o que evite el almacenamiento de nuevos archivos en estos dispositivos. El acceso a las redes inalámbricas puede ser controlado en el punto final. Dos tipos de control están disponibles:</p> <ol style="list-style-type: none"> 1 - Especificar los tipos de conexión a los que se permite el acceso 2 - Determinar las redes específicas a las cuales se permite el acceso.
DS11 Administración de datos		
DS11.3 Sistema de administración de librerías de medios	Mantener un inventario de los medios de almacenamiento que permita definir su usabilidad y su integridad.	Aranda 360 ENDPOINT SECURITY permite obtener información sobre todos los dispositivos removibles de almacenamiento conectados a un punto final. El reporte también identifica el tipo de dispositivo utilizado.
DS11.6 Requerimientos de seguridad para la administración de datos	Se deben implementar controles para hacer cumplir los requisitos para el manejo de la información. Esto incluye todos los dispositivos removibles de almacenamiento que sean retirados fuera de la organización.	Aranda 360 habilita controles de acceso permitiendo acceso total, bloqueo o acceso de sólo lectura para cualquier dispositivo identificado como dispositivo de almacenamiento (memorias USB, cámaras digitales, unidades de floppy, CD ó DVD, discos duros externos y teléfonos celulares).
DS12 Administración del ambiente físico		

<p>DS12.4 Protección contra factores ambientales</p>	<p>Se deben implementar contramedidas que permitan mitigar las amenazas físicas del ambiente. Esto debe incluir controles tanto de prevención como de detección.</p>	<p>Existen muchas amenazas físicas para los medios removibles. Estas incluyen el robo, deshecho inapropiado y pérdida accidental del medio. Es importante asegurar que la información contenida en los medios se encuentra protegida cuando estas amenazas se materializan. Aranda 360 asegura que toda la información almacenada en los medios removibles se encuentra encriptada en caso de robo o pérdida.</p>
<p>DS13 Administración de operaciones</p>		
<p>DS13.3 Monitoreo de la infraestructura de TI</p>	<p>Cualquier implementación de monitoreo debe contener información suficiente para permitir la reconstrucción histórica de cualquier evento relacionado con la seguridad.</p>	<p>Aranda 360 crea un <i>log</i> de auditoría para ciertas actividades en el punto final. Cada entrada de este registro tiene una fecha y hora asociadas. Desde la consola se pueden aplicar filtros de <i>logs</i> y ordenar los registros en orden cronológico. Los <i>logs</i> también pueden ser exportados para análisis posteriores.</p>
<p>ME2 Monitorear y evaluar el control interno</p>		
<p>ME2.2 Revisión de Auditoría</p>	<p>El entorno de TI y los controles deben ser monitoreados continuamente.</p>	<p>Los eventos que ocurren en puntos finales protegidos por Aranda 360 son almacenados en <i>logs</i> y alertas. Estos registros contienen información detallada, tal como el nombre de un archivo accedido a través de un medio removible o almacenado en este. Adicionalmente a los eventos que ocurren en los puntos finales, Aranda 360 crea registros de auditoría de todas las acciones de administración realizadas a través de la consola de administración. Todos estos registros son enviados al servidor de base de datos para su almacenamiento y podrán ser consultados por cualquier administrador en cualquier momento.</p>
<p>AC Controles de origen de datos/ autorización</p>		
<p>AC18 Protección de información sensible durante su transmisión y</p>	<p>Se deben implementar controles para proteger la integridad y</p>	<p>Con Aranda 360 ENDPOINT SECURITY es posible implementar control de acceso</p>

<p>transporte</p>	<p>confidencialidad de información sensible durante su transmisión y transporte.</p>	<p>y encriptación en el punto final. Esto es utilizado para asegurar que:</p> <ol style="list-style-type: none"> 1- Los permisos de acceso a archivos estén definidos. - Ej. Solo lectura. 2- La encriptación de datos se aplique a todo tipo de información confidencial. 3- Asegurar que se utilicen redes inalámbricas seguras para la transmisión de información sensible.
-------------------	--	---

CONCLUSIONES

Las tecnologías móviles han creado nuevos desafíos para el cumplimiento de SOX.

La seguridad tradicional tiene serias limitaciones - un perímetro de información con puntos de control de acceso localizados ya no puede evitar la fuga de datos-. Las tecnologías más recientes pueden saltarse esta barrera y transferir información sin tener controles de acceso definidos. El cumplimiento de SOX sigue siendo una prioridad alta en cualquier organización de seguridad. Sin embargo, las empresas quieren aprovecharse de la mejoras de productividad que estas nuevas tecnologías móviles ofrecen. Al poner en una balanza estas necesidades contrarias entre sí, resulta un constante dilema para los profesionales de TI.

Aranda 360 ENDPOINT SECURITY refuerza las protecciones existentes y se integra con las soluciones de acceso existentes en la organización para controlar el flujo de información desde cualquier punto final. Esto aborda la difícil tarea de asegurar que la fuga de información tenga un impacto mínimo sobre el cumplimiento de SOX. Aranda 360 también proporciona herramientas para administrar los componentes de protección y los requerimientos de auditoría. Además, los controles técnicos se pueden integrar fácilmente con las políticas y procedimientos existentes - obteniendo como resultado controles que pueden ser rentables y de rápida implementación. Sin este tipo de contramedidas de seguridad, las organizaciones se enfrentan a graves brechas en toda la infraestructura diseñada para ser compatible con SOX.