

# **Aranda 360 ENDPOINT SECURITY**

**CORRESPONDENCIA CON LA CIRCULAR N° G-140-2009**

**SUPERINTENDENCIA DE BANCA Y SEGUROS DE PERÚ**

**Gestión de la Seguridad de la Información**



**Ámbito de aplicación de acuerdo a la Circular**

De acuerdo al Artículo 1º de la circular, las disposiciones de esta norma son aplicables a las empresas señaladas en los artículos 16º y 17º de la Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, a las Administradoras Privadas de Fondos de Pensiones (AFP), a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., y las Derramas y Cajas de Beneficios bajo control de la Superintendencia, la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC) y el Fondo de Cajas Municipales de Ahorro y Crédito (FOCMAC), en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas. **Aranda 360 ENDPOINT SECURITY** cumple como solución de implementación de los objetivos de control y requerimientos establecidos en los artículos 4 (Estructura organizacional) y 5 (Controles de seguridad de información), como se describen a continuación:

**Artículo 4: Estructura organizacional**

Las empresas deben contar con una estructura organizacional que les permita implementar y mantener el sistema de gestión de la seguridad de información señalado en el artículo anterior.

Asimismo, deben asegurarse que se desarrollen las siguientes funciones, ya sea a través de una unidad especializada o a través de alguna de las áreas de la empresa.

Lo que dice la Circular	Lo que hacemos
<p><b>.a.</b> Asegurar el cumplimiento de la política de seguridad de información y de la metodología definida.</p>	<p><b>Aranda 360 ENDPOINT SECURITY</b> es una solución enfocada a reforzar el cumplimiento de las políticas de seguridad y uso de las entidades vigiladas por la Superintendencia de Banca y Seguros. La consecuente aplicación de la política de seguridad garantiza la permanente disponibilidad de los recursos informáticos y la integridad de la información como principal activo de las entidades.</p>
<p><b>.b.</b> Coordinar y monitorear la implementación de los controles de seguridad de información.</p>	<p><b>Aranda 360 ENDPOINT SECURITY</b> pone a disposición controles que permiten monitorear el uso de los recursos informáticos y auditar todo tipo de eventos relacionados con la seguridad del sistema y de las comunicaciones en cada punto final de la infraestructura informática.</p>

**Artículo 5: Controles de seguridad de información**

Como parte de su sistema de gestión de la seguridad de información, las empresas deberán considerar, como mínimo, la implementación de los controles generales que se indican en el presente artículo.



<b>5.1. Seguridad Lógica</b>	
<b>Lo que dice la Circular</b>	<b>Lo que hacemos</b>
<b>.d.</b> Controles especiales sobre utilidades del sistema y herramientas de auditoría.	Implementar controles y restricciones en la ejecución de aplicaciones y utilidades del sistema operativo.  Implementar auditoría sobre los accesos controlados y eventos relacionados con la protección del sistema, dispositivos y comunicaciones de red.
<b>.e.</b> Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.	Reportar actividades relacionadas con accesos no autorizados, intentos de violación de los controles establecidos
<b>.f.</b> Controles especiales sobre usuarios remotos y computación móvil.	Implementar controles y políticas de seguridad persistentes independientemente del estado de conectividad. Aplicar políticas dinámicas de acuerdo al tipo de infraestructura y conectividad de red.
<b>5.5. Administración de las operaciones y comunicaciones</b>	
<b>.g.</b> Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.	Implementar controles y protecciones contra códigos maliciosos, software espía, rootkits y malware en general conocido y desconocido.
<b>.h.</b> Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.	Implementar un firewall de red a nivel de host que permite filtrar tráfico de red entrante y saliente, adicional a un sistema de prevención de intrusiones que detecta comportamientos sospechosos y ataques de red especializados.  Implementar controles de uso de dispositivos removibles de almacenamiento y acceso a los archivos contenidos.
<b>.i.</b> Seguridad sobre el intercambio de la información, incluido el correo electrónico.	Aplicar controles sobre el tipo de archivos que pueden ser adjuntados o accedidos a través del correo electrónico.  Restringir o controlar las transferencias de archivos a través de programas de mensajería instantánea, clientes FTP, y navegadores Web.
<b>.j.</b> Seguridad sobre canales electrónicos.	Controlar el acceso a la red por parte de las aplicaciones- Forzar el uso de canales y/o protocolos de comunicación seguros en conexiones inalámbricas y externas a la red corporativa.
<b>.k.</b> Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas.	Registrar todo tipo de actividad relacionada con los controles establecidos, ataques de seguridad y operaciones de acceso a archivos y a las

	<p>aplicaciones.</p> <p>Monitorear el estado de conectividad y seguridad de los puntos finales.</p> <p>Registrar todas las operaciones de administración y gestión realizadas por los administradores de <b>Aranda 360 ENDPOINT SECURITY</b>.</p>
<p><b>5.6 Adquisición, desarrollo y mantenimiento de sistemas informáticos</b></p> <p>Para la administración de la seguridad en la adquisición, desarrollo y mantenimiento de sistemas informáticos, se debe tomar en cuenta, entre otros, los siguientes criterios:</p>	
<p><b>.b.</b> Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.</p>	<p>Implementar políticas de encriptación en dispositivos removibles de almacenamiento y en discos duros fijos.</p>
<p><b>.c.</b> Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.</p>	<p>Aplicar políticas de control de aplicaciones en modo prueba para comprobar la seguridad y protección antes de su puesta en producción.</p>
<p><b>.f.</b> Controlar las vulnerabilidades técnicas existentes en los sistemas de la empresa.</p>	<p>Prevenir el aprovechamiento de las vulnerabilidades del sistema operativo y de cualquier software instalado.</p> <p>Proteger contra ataques específicamente diseñados para explotar vulnerabilidades o defectos en las aplicaciones y el sistema operativo.</p>