

**Aranda 360 ENDPOINT SECURITY
CORRESPONDENCIA CON LA CIRCULAR
EXTERNA 052 DE 2007
SUPERINTENDENCIA FINANCIERA DE COLOMBIA**



Mayo 2008

CAPITULO DECIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN A TRAVÉS DE MEDIOS Y CANALES DE DISTRIBUCIÓN DE PRODUCTOS Y SERVICIOS

Ámbito de aplicación de acuerdo a la Circular

Las instrucciones de que trata este capítulo deberán ser adoptadas por todas las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC), con excepción de las siguientes: el Fondo de Garantías de Instituciones Financieras “Fogafín”, el Fondo de Garantías de Entidades Cooperativas “Fogacoop”, el Fondo Nacional de Garantías S.A. “F.N.G. S.A.”, el Fondo Financiero de Proyectos de Desarrollo “Fonade”, los Almacenes Generales de Depósito, los Fondos de Garantía que se constituyan en el mercado público de valores, los Fondos Mutuos de Inversión, los Fondos Ganaderos, las Sociedades Calificadoras de Valores y/o Riesgo, las Oficinas de Representación de Instituciones Financieras y de Reaseguros del Exterior, los Corredores de Seguros y de Reaseguros, los Comisionistas Independientes de Valores, las Sociedades Comisionistas de Bolsas Agropecuarias y los Organismos de Autorregulación.

Aranda 360 ENDPOINT SECURITY cumple como solución de implementación de los objetivos de control y requerimientos establecidos en los numerales 3.1.1, 3.1.4, 3.1.5, 3.1.7, 3.1.11, 3.1.14 y 3.1.17 (Seguridad y Calidad) y en los numerales 4.7.2, 4.7.3, 4.7.4, 4.7.5 (Centro de Atención Telefónica Call Center), como se describen a continuación:

<p>3.1 SEGURIDAD Y CALIDAD</p> <p>En desarrollo de los criterios de seguridad y calidad, y considerando los canales de distribución utilizados, las entidades deberán cumplir, como mínimo, con los siguientes requerimientos:</p>	
Lo que dice la Circular	Lo que hacemos
<p>3.1.1</p> <p>Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información en condiciones de seguridad y calidad.</p>	<p>Aranda 360 ENDPOINT SECURITY pone a disposición de las entidades reguladas por la Superintendencia Financiera de Colombia una solución de software que protege las organizaciones de los ataques informáticos externos e integra la definición de políticas adecuadas para el uso de los puntos finales (estaciones de trabajo y laptops).</p> <p>Con Aranda 360 es posible asegurar los datos y archivos importantes y críticos de la entidad, además de la información confidencial mediante el bloqueo de las amenazas de red, uso de dispositivos removibles y detección de software malicioso.</p>

<p>3.1.4</p> <p>Dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la entidad.</p>	<ul style="list-style-type: none"> • Encriptar los datos almacenados en dispositivos removibles. • Definir zonas de encriptación en discos duros (archivos y directorios) y controlar el acceso mediante uso de contraseñas • Establecer permisos de acceso a registros y archivos.
<p>3.1.5</p> <p>Velar por que la información enviada a los clientes esté libre de software malicioso.</p>	<ul style="list-style-type: none"> • Proteger el sistema contra software dañino (gusanos y virus). • Defender al sistema de programas espía (troyanos, spyware, keyloggers, rootkits).
<p>3.1.7</p> <p>Dotar a sus terminales o equipos de cómputo de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones.</p>	<ul style="list-style-type: none"> • Restringir la instalación de software no autorizado y la desinstalación de aplicaciones existentes. • Proteger el sistema contra la ejecución de keyloggers y software espía. • Restringir el uso de dispositivos removibles (USB, Firewire, COM, IrDA, PCMCIA) mediante la identificación del fabricante, número serial o modelo del dispositivo.
<p>3.1.11</p> <p>Establecer los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo solo lo pueda realizar personal debidamente autorizado.</p>	<ul style="list-style-type: none"> • Permitir la instalación y/o desinstalación de software, acceso a las herramientas del panel de control de Windows y el acceso a las utilidades de administración del sistema operativo (Administrador de tareas, Editor del registro, etc.), únicamente a usuarios autorizados identificados.

<p>3.1.14</p> <p>Realizar una adecuada segregación de funciones del personal que administre, opere, mantenga y, en general, tenga la posibilidad de acceder a los dispositivos y sistemas usados en los distintos canales y medios de servicio al cliente y al usuario. En desarrollo de lo anterior, las entidades deberán establecer los procedimientos y controles para el alistamiento, transporte, instalación y mantenimiento de los dispositivos usados en los canales de distribución de servicios.</p>	<ul style="list-style-type: none"> • Encriptar los datos almacenados en dispositivos removibles. • Controlar las operaciones de acceso y modificación de archivos almacenados en dispositivos de almacenamiento removibles.
<p>3.1.17</p> <p>Tener en operación solo los protocolos, servicios, aplicaciones, usuarios, equipos, entre otros, necesarios para el desarrollo de su actividad.</p>	<ul style="list-style-type: none"> • Controlar las aplicaciones de los usuarios mediante el acceso a listas blancas y listas negras. • Establecer permisos de acceso detallados para cada aplicación. • Establecer permisos de acceso a registros y archivos. • Detectar accesos no autorizados a un computador o a una red mediante el IDS (sistema de detección de intrusos). • Filtro avanzado de tráfico (protocolos múltiples sobre IP, TCP/UDP/ICMP y Ethernet, y filtro de direcciones MAC/IP). • Revisar la integridad del protocolo. • Proteger la red del escaneo de puertos. • Controlar el tráfico de red en los puntos finales de acuerdo a los niveles de servicio mediante un firewall integrado al kernel.

Lo que dice la Circular	Lo que hacemos
<p>4.7.2</p> <p>Impedir el ingreso de dispositivos que permitan almacenar o copiar cualquier tipo de información, o medios de comunicación, que no sean suministrados por la entidad.</p>	<ul style="list-style-type: none"> • Restringir la copia de archivos a unidades de almacenamiento externo, quemadoras de CD/DVD, memorias USB, discos duros externos. • Permitir el acceso a dispositivos autorizados por la entidad identificados por su fabricante, número serial o modelo.
<p>4.7.3</p> <p>Dotar a los equipos que operan en el centro de atención telefónica de los elementos necesarios que impidan el uso de dispositivos de almacenamiento no autorizados por la entidad. Igualmente, se deberá bloquear cualquier tipo de conexión a red distinta a la usada para la prestación del servicio.</p>	<ul style="list-style-type: none"> • Restringir el uso de dispositivos removibles de almacenamiento no autorizados o identificados previamente por la entidad. • Controlar las conexiones a redes inalámbricas (Infraestructura y Ad-Hoc). • Controlar las conexiones inalámbricas de acuerdo a la identificación (SSID, MAC), y a los métodos de encriptación y autenticación de los puntos de acceso (WEP, WPA, WPA2, etc.). • Proteger las configuraciones de red de los puntos finales de cualquier modificación hecha por el usuario. • Restringir conexiones Bluetooth. • Controlar perfiles de conectividad inalámbrica (Conexión LAN, hotspots, VPN, etc.). • Permitir el acceso remoto a los recursos de la red mediante el uso de herramientas de conexión VPN autorizadas.
<p>4.7.4</p> <p>Garantizar que los equipos destinados a los</p>	<ul style="list-style-type: none"> • Ejecutar scripts de verificación de procesos de las soluciones de

<p>centros de atención telefónica solo serán utilizados en la prestación de servicios por ese canal.</p>	<p>seguridad y de otro software de seguridad.</p> <ul style="list-style-type: none"> • Monitorear actividades y generar reportes permanentemente. • Generar alertas sobre actividades irregulares o incidentes de seguridad en tiempo real. • Controlar el acceso a las aplicaciones mediante el uso de listas de control de acceso (ACL). • Establecer permisos de acceso detallados para cada aplicación. • Configurar permisos de acceso a la red. • Agrupar y administrar redes de puntos finales identificados mediante membresía en Active Directory, dirección IP, segmento de red y dirección MAC. • Restringir el acceso al sistema de administración de usuarios y evitar la modificación de los niveles de acceso.
<p>4.7.5</p> <p>En los equipos usados en los centros de atención telefónica no se permitirá la navegación por Internet, el envío o recepción de correo electrónico, la mensajería instantánea, ni ningún otro servicio que permita el intercambio de información, a menos que se cuente con un sistema de registro de la información enviada y recibida. Estos registros deberán ser conservados por lo menos un (1) año o en el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.</p>	<ul style="list-style-type: none"> • Impedir la navegación mediante la restricción de acceso a los puertos HTTP, HTTPS para cualquier navegador web, así mismo como la descarga de cualquier tipo de archivo. • Restringir la ejecución de clientes de correo, la conexión a puertos utilizados por protocolos de correo (SMTP, IMAP, POP3, etc). • Restringir la ejecución de clientes de mensajería instantánea e impedir la transferencia de archivos a través de estos.