

# ARANDA 360 ENDPOINT SECURITY

CORRESPONDENCIA CON LA CIRCULAR RUNOR 1-805  
(Comunicaciones "A" 4690 y "B" 9042)

Requisitos mínimos de gestión, implementación y control de los riesgos  
Relacionados con tecnología informática y sistemas de información

Banco Central De La República Argentina



**Ámbito de aplicación**

De acuerdo a las comunicaciones “A” 4690 y “B” 9042 emitidas en 27/12/2006 y en 24/07/2007 respectivamente por el Banco Central de la República Argentina, se aprueban las normas sobre “Requisitos Mínimos de Gestión, Implementación y Control de los Riesgos Relacionados con Tecnología Informática, Sistemas de Información y Recursos Asociados para las Entidades Financieras”. Las disposiciones de esta norma enumeran una serie de requisitos mínimos que las entidades financieras deberán cumplir, los que serán sometidos a supervisión por parte de la Superintendencia de Entidades Financieras y Cambiarias.

Aranda 360 ENDPOINT SECURITY cumple como solución de implementación de los objetivos de control y requerimientos establecidos en la sección 3 (Protección de Activos de Información), como se describen a continuación:

<p><b>Numeral 3.1.4: Política de Protección</b></p> <p><i>“De acuerdo con su estrategia de seguridad, las entidades financieras deben desarrollar una política de protección de los activos de información. Ésta debe evidenciar claramente que es un instrumento que se utiliza para proporcionar dirección y apoyo gerencial con el objeto de brindar protección de los activos de información. Además, identificará los recursos críticos a proteger y los riesgos internos y externos de accesos no autorizados sobre los mismos.”</i></p>	
<p><b>Lo que dice la Circular</b></p>	<p><b>Lo que hacemos</b></p>
<p><b>3.1.4.3 Programas de utilidad con capacidades de manejo de datos - Usuarios privilegiados y de contingencia.</b></p> <p>Deben implementarse adecuadas restricciones para el empleo de los programas que permitan el alta, la baja o la modificación de datos operativos por fuera de los sistemas aplicativos, en las distintas plataformas.</p> <p>Asimismo, deben desarrollarse mecanismos formales para la asignación y la utilización de usuarios especiales con capacidades de administración, que puedan ser usados en caso de emergencia o interrupción de las actividades. Los usuarios definidos con estas características deben contar con adecuadas medidas de resguardo y acceso restringido. Su utilización será registrada y se realizarán controles posteriores sobre los reportes de eventos, analizando la concordancia entre las tareas realizadas y el motivo por el cual se los solicitó.</p>	<ul style="list-style-type: none"> <li>• Controlar el acceso a las aplicaciones.</li> <li>• Establecer permisos de acceso detallados para cada aplicación.</li> <li>• Restringir el acceso al sistema de administración de usuarios y evitar la modificación de los niveles de acceso.</li> <li>• Proteger el sistema de la ejecución de <i>rootkits</i> que intentan elevar los privilegios del usuario.</li> </ul>



<p><b>3.1.4.4. Registros de seguridad y pistas de auditoría.</b></p> <p>Con el objeto de reducir a un nivel aceptable los riesgos internos y externos de accesos no autorizados, pérdidas y daños a la información, se deben implementar adecuadamente:</p> <ul style="list-style-type: none"> <li>• Registros operativos de las actividades de los usuarios, las tareas realizadas y las funciones utilizadas.</li> <li>• Reportes de seguridad que registren la asignación de claves y derechos de accesos, empleo de programas de utilidad que permitan el manejo de datos por fuera de las aplicaciones, actividades de los usuarios privilegiados, usuarios de emergencia y con accesos especiales, intentos fallidos de acceso y bloqueos de cuentas de usuario, y reportes de auditoría que registren las excepciones y actividades críticas de las distintas plataformas.</li> </ul>	<ul style="list-style-type: none"> <li>• Monitorear y registrar actividades relacionadas con el uso de las aplicaciones, acceso a los archivos, acceso a recursos de la red y uso de dispositivos removibles.</li> <li>• Auditar todo tipo de eventos relacionados con intentos fallidos de acceso a los recursos restringidos por la política de seguridad.</li> <li>• Generar reportes gráficos sobre el estado de integridad y seguridad de los puntos finales asimismo como de los usos y bloqueos más frecuentes a los recursos del sistema controlados por las políticas de seguridad.</li> </ul>
<p><b>3.1.4.5. Alertas de seguridad y software de análisis.</b></p> <p>Las entidades financieras deben implementar funciones de alertas de seguridad y sistemas de detección y reporte de accesos sospechosos a los activos de información, y contar con monitoreo constante de los accesos a recursos y eventos críticos, que reporten a los administradores sobre un probable incidente o anomalía en los sistemas de información.</p> <p>Asimismo, se considera una sana práctica de seguridad la detección en tiempo real de los eventos o intrusiones, así como la utilización de herramientas automatizadas para el análisis de la información contenida en los registros operativos, de seguridad y de auditoría. De esta manera, se reducirá el volumen de los datos contenidos en los reportes, minimizando los costos relacionados con su almacenamiento y tareas de revisión.</p>	<ul style="list-style-type: none"> <li>• Generar alertas sobre actividades irregulares o incidentes de seguridad en tiempo real.</li> <li>• Almacenar y exportar alertas y registros de actividades a sistemas externos de análisis y generación de reportes. (Correlacionadores, Syslog, SMTP, etc.).</li> <li>• Detectar acciones sospechosas y peligrosas mediante un sistema de detección de intrusiones a nivel de host (HIPS).</li> <li>• Personalizar el registro y el análisis de los eventos de seguridad con el fin de optimizar la calidad y cantidad de la información de auditoría.</li> </ul>

<p><b>3.1.4.6. Software malicioso.</b></p> <p>Las entidades financieras deben implementar adecuados mecanismos de protección contra programas maliciosos, tales como: virus informáticos, “gusanos” de red, “spyware”, “troyanos”, y otros que en el futuro puedan surgir, con el objeto de prevenir daños sobre los datos y la pérdida de información. Deben desarrollar procedimientos de difusión a los usuarios de los sistemas de información y a los recursos humanos de las áreas técnicas, sobre sanas prácticas en materia de prevención.</p> <p>Deben implementarse herramientas para la prevención, detección y eliminación de este tipo de software en los distintos ambientes de procesamiento, evitando su propagación y replicación a través de las redes informáticas, archivos y soportes de información. Estas herramientas deben actualizarse rutinariamente contra nuevas amenazas.</p> <p>Deberán definirse controles de seguridad para prevenir la presencia de código malicioso en archivos adjuntos a correos electrónicos y en los accesos a Internet; asimismo, se deberá impedir la instalación y utilización de software no autorizado.</p>	<ul style="list-style-type: none"> <li>• Proteger el sistema contra ataques conocidos y desconocidos, ataques de Día-0 y contra códigos maliciosos sin firmas digitales.</li> <li>• Proteger el sistema contra software dañino (gusanos y virus).</li> <li>• Restringir la acción peligrosa de programas espía mediante la detección y bloqueo de <i>keyloggers</i> y <i>rootkits</i>.</li> <li>• Proteger el uso de recursos críticos contra ataques de desbordamientos de memoria, reinicios espontáneos y uso excesivo de CPU.</li> <li>• Restringir la instalación de software y la modificación binaria de aplicaciones ya existentes.</li> <li>• Controlar el uso de archivos adjuntos en correos electrónicos y en las descargas a través de la navegación web.</li> <li>• Detectar comportamientos anormales en las comunicaciones de red mediante el análisis de los protocolos utilizados en las conexiones.</li> <li>• Protección contra ataques de red sofisticados (Denegación de Servicio, Inundaciones IP, Análisis de Puertos, Suplantación ARP).</li> </ul>
---	--