Principios para reforzar la seguridad de la información en el sistema financiero

1. **Gobierno corporativo en el que la seguridad informática ocupe un lugar central**: las entidades deben contar con una unidad administrativa en los niveles más altos de la organización, que defina políticas y estrategias, conforme a las mejores prácticas y estándares internacionales, y sea responsable de la seguridad de la información de la entidad.

2. **Esquemas de protección de datos robustos**: contar con mecanismos y procesos para una gestión segura de todos los activos de información de la entidad; independiente de si dicha información se almacena en medios electrónicos o físicos.

3. **Administración de riesgos de seguridad de la información**: la metodología de administración de riesgos de la entidad, deberá contar con un apartado específico de medición y gestión de riesgos de seguridad de la información.

4. **Controles de seguridad en los puntos de acceso**: los procedimientos de acceso a dispositivos, equipos y servidores deberán contemplar esquemas de gestión de claves, permisos y roles; que garanticen que sólo pueden acceder quienes lo requieren y por el tiempo que lo requieren. Así mismo, se deberá contar con herramientas que controlen y monitoreen el acceso a dispositivos, equipos y servidores.

5. **Protocolos de respuesta a incidentes y eventos críticos**: las entidades deberán contar con procedimientos claros y documentados para responder ante un incidente que vulnere sus mecanismos de protección, y considerar en dichos protocolos escenarios donde, con motivo del incidente, el impacto escale a nivel sistémico, dentro o fuera de la entidad.

6. **Identificación de exposición a riesgos por parte de terceros (proveedores y usuarios)**: las entidades deberán asegurarse que sus proveedores de servicios y aplicaciones cumplen con niveles de seguridad de la información conforme a las políticas que defina su órgano de gobierno de la seguridad de la información.

7. **Políticas de protección a la infraestructura**: los centros de datos, así como la infraestructura de cómputo y de telecomunicaciones deberá ser gestionada conforme a las mejores prácticas y estándares de seguridad de la industria; y en apego a las políticas que defina el órgano de gobierno de la seguridad de la información de la entidad.

8. **Políticas de protección a los sistemas**: las aplicaciones, bases de datos y sistemas informáticos con que cuente la entidad deberán estar protegidos y gestionados de forma segura, conforme a las mejores prácticas y estándares internacionales, y en apego a las reglas que defina el órgano de seguridad de la información.

9. **Programa de capacitación y de fomento de una cultura de la seguridad informática**: el personal deberá estar capacitado y ser consciente de que la protección de la información es responsabilidad de cada empleado; las áreas de tecnología, ciberseguridad o de políticas de seguridad de la información, proveen herramientas o lineamientos, pero es responsabilidad de cada individuo conocer la criticidad de la información que maneja y protegerla concordancia.

10. **Programas de educación y fomento de una cultura de seguridad informática para el uso que hacen los clientes de los servicios financieros:** Las instituciones deberán redoblar sus esfuerzos para promover entre sus clientes un pleno conocimiento de sus aplicativos y las prácticas de seguridad que deben de seguir.