19. POLÍTICA DE SEGURIDAD DE PROVEEDORES.

19.1. Implementación de la política

Las Políticas de Seguridad de la Información son de aplicación obligatoria para toda persona que, vinculada contractualmente o suministrada por un tercero, realice labores como proveedor del FNA, independiente del área o compañía a la cual pertenezca y cualquiera sea el nivel de las tareas que desempeñe.
Así mismo, los funcionarios de FNA que interactúen con un proveedor, o que sean responsables de la supervisión de su actividad, deben
tomar conciencia acerca de los temas relacionados con la seguridad de la información, y deberán propender para que se utilicen los controles pertinentes y se sigan con los procedimientos definidos antes, durante, y después de la relación contractual con el proveedor. Es
responsabilidad de dichos funcionarios que los proveedores cumplan con lo establecido en el presente Manual de Políticas De Seguridad
de la Información.

19.2. Acuerdos de confidencialidad

Toda relación contractual que establezca una persona natural o jurídica con el FNA deberá incluir un acuerdo de confidencialidad y una cláusula de cumplimiento de la política de seguridad de la información, y se debe incluir que el FNA podrá auditar el cumplimiento de lo
establecido en dichos documentos, así como las penalizaciones con base en los daños potenciales ante la violación de la confidencialidad
de la información.
En este sentido, se debe dar cumplimiento a los lineamientos dados por la Política de acuerdos de confidencialidad y de no divulgación del
FNA.

19.3. Protección de datos personales

Se debe incluir dentro de los C ontratos una cláusula que haga referencia al cumplimiento de la Política de protección de Datos Personales
del FNA, documento que debe ser entregado al Proveedor para su entendimiento y aceptación.

19.4. Control y Auditoría

Los dueños de la información deberán propender por que los proveedores y personal de terceros que realizan funciones sobre la información de la Entidad generen los registros de auditoría sobre cualquier acción en los activos de información. Los dueños de la información son los responsables por los riesgos asociados a las acciones de los proveedores en los activos de información a su cargo, por ello deben propender porque existan los acuerdos, controles y revisiones pertinentes.
El supervisor o interventor del contrato será el responsable de verificar el cumplimiento de las condiciones de seguridad de la información
formalizadas en los acuerdos establecidos. A su vez, el Grupo de Seguridad de la Información deberá revisar periódicamente que estas
verificaciones en efecto se lleven a cabo.
El supervisor o interventor del contrato, será responsable de definir las acciones que se tomarán cuando se observen situaciones que atenten contra la seguridad de la información (Integridad, C onfidencialidad, Disponibilidad) en los servicios o productos suministrados por
los terceros, de acuerdo con los lineamientos del contrato. En todo caso, deberá reportar la situación como un evento de acuerdo al Procedimiento Gestión De Incidentes.

19.5. Gestión de incidentes

Es obligación por parte de los funcionarios de la empresa proveedora el reporte de cualquier anomalía que sea detectada para que su tratamiento sea oportuno y se prevengan incidentes de Seguridad. El reporte debe ser canalizado a través de los diferentes niveles jerárquicos hasta llegar al punto de contacto directo con el FNA, quien lo reportará al supervisor del contrato, quien a su vez lo reportará
a la Mesa de Servicio a través del Procedimiento Gestión De Incidentes

19.6. Requerimientos de Seguridad de Aplicaciones y/o servicios

Si el proveedor es responsable por aplicaciones o servicios informáticos estos deben cumplir con los requerimientos de protección de la
C onfidencialidad, Integridad y Disponibilidad definidos por el FNA, y que debe demostrar con base en el activo que va a ser manejado con
uno o más de los siguientes controles:

- **Monitoreo:** Estar en capacidad de brindar los mecanismos para detectar incidentes de seguridad de la información sobre el funcionamiento de la aplicación con el que se presta el servicio al FNA. El nivel de detección se ajustará a los requerimientos del activo
involucrado en el servicio.
- **Gestión de Vulnerabilidades:** Mantener un proceso de revisión permanente de las posibles vulnerabilidades en las aplicaciones que
son responsabilidad del proveedor y establecer el proceso de asesoría hacia el FNA, con el fin de mitigar oportunamente los riesgos asociados con las vulnerabilidades identificadas.
- **Control de acceso:** Presentar los mecanismos de control de acceso a los servicios y los datos manejados con base en la Política de C ontrol de Acceso del FNA.
- **Gestión de incidentes:** C ontar con un esquema de identificación, reporte, escalamiento, tratamiento y documentación de los incidentes que se presenten en el funcionamiento de la aplicación o servicio prestado.
- **Soporte:** El proveedor debe contar con los expertos idóneos para atender incidentes o eventos de seguridad de la información con base en el SGSI del FNA.
- **Redundancia:** Si los servicios provistos así lo requieren, el proveedor debe contar con sistemas redundantes que le permitan cumplir
con los acuerdos de niveles de servicio acordados con el FNA.
- **Licenciamiento:** Todas las aplicaciones y servicios prestados por el proveedor deben contar con el licenciamiento acorde con el marco
legal y regulaciones que apliquen al FNA.

19.7. Requerimientos de Seguridad de la Información de la Empresa Proveedora

El FNA exigirá unas condiciones mínimas con respecto a Seguridad de la Información para las empresas proveedoras con las que exista
intercambio de información catalogada como Pública C lasificada y Pública Reservada. Así mismo la que este definida en nivel Muy Alto

para Integridad y Disponibilidad, a saber:
• C ontar con un sistema de gestión de seguridad de la información.
• Presentar la política de seguridad de la información referente al servicio o producto que se está prestando al FNA.
• Presentar el soporte para el procedimiento de tratamiento de los incidentes de seguridad de la información que puedan darse en el desarrollo del servicio o el producto entregado.
• Mostrar sus procedimientos de gestión de vulnerabilidades y diagnóstico de seguridad.
• Mostrar los planes de contingencia y recuperación donde muestre su capacidad de cumplir con la disponibilidad exigida en los acuerdos
de niveles de servicio.
Las empresas proveedoras cuyos servicios incluyen aspectos controlados por la legislación o regulaciones vigentes aplicables al FNA, deben asegurar y demostrar su cumplimiento.

19.8. Términos y condiciones

El proceso de C ontratación deberá establecer en los contratos las limitaciones necesarias para que el proveedor cumpla las políticas, los
procedimientos y los instructivos de la seguridad de la información del FNA.
Todos los contratos, en materia de seguridad de la información, deberán incluir como mínimo lo siguiente:

19.8.1. C umplimiento de las políticas de seguridad de la información y de la política de protección de datos personales del FNA por parte
del tercero.
19.8.2. Niveles de servicio y operación.
19.8.3. Acuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas.
19.8.4. Propiedad de la información.
19.8.5. Restricciones sobre el software empleado.
19.8.6. Normas de seguridad física a ser aplicadas.
19.8.7. Procedimientos o instructivos a seguir cuando se encuentre evidencia de alteración o manipulación de equipos o información.
19.8.8. Procedimientos o instructivos y controles para la entrega de la información manejada y la destrucción de la misma por parte del

COPIA CONTROLADA

tercero una vez finalizado el servicio.
19.8.9. Documentación de los controles físicos y lógicos empleados por el tercero para proteger la confidencialidad, integridad, disponibilidad de los datos y los equipos.
19.8.10. Los requisitos para la protección de los datos privados acorde a la ley.
19.8.11. El cumplimiento explícito de la normatividad vigente y aplicable al FNA, en materia de seguridad de la información.
19.8.12. Responsabilidades de confidencialidad de la información posteriores a la terminación del contrato.
19.8.13. Responsabilidades y sanciones en caso de incumplimiento de los acuerdos respectivos.