APROBADO MEDIANTE ACUERDO 2460 de 2022

TABLA DE CONTENIDO

COPIA

3. ALCANCE

Este manual de políticas para la seguridad de la información aplica en todo el ámbito del FNA, en el desarrollo de gestión que incluye el Talento Humano, los recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros que involucren manejo de información catalogada como clasificada o reservada o sean considerados como terceros críticos para la Entidad, los cuales deberán cumplir como mínimo con las obligaciones descritas en la Política de Seguridad de Proveedores, y de acuerdo con la naturaleza y complejidad del servicio prestado.

Todos los empleados, temporales, contratistas, practicantes, terceros o cualquier persona que tenga una relación contractual con la Entidad, o que tengan acceso a los activos de información del FNA, sea cual fuere su nivel jerárquico, son responsables de la aplicación de las políticas definidas en este manual dentro de sus áreas de responsabilidad, así como del cumplimiento por parte de su grupo de trabajo.

Las Políticas de Seguridad de la Información son de aplicación obligatoria para toda persona vinculada contractualmente, así como los recursos suministrados por terceros proveedores con el FNA que involucren manejo de información catalogada como clasificada o reservada, el área a la cual pertenezca y cualquiera sea el nivel de las tareas que desempeñe.

A nivel de Seguridad de la Información, lo que no está definido en el presente manual, se entiende como prohibido.

Para implementar el sistema para la seguridad de la información en la entidad, se han definido los siguientes roles y sus respectivas responsabilidades.

19. POLÍTICA DE SEGURIDAD DE PROVEEDORES.

COPIA CONTROLADA

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, los controles de seguridad de la información a tener en cuenta deberán contemplar las actividades que desarrollará el proveedor y el nivel de clasificación de la información a la cual podría tener acceso en la ejecución del acuerdo contractual.

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 niveles de servicio y operación

Según lo previsto en la Circular Básica Jurídica de la Superintendencia Financiera de Colombia, cuando se contrate bajo la modalidad de outsourcing o tercerización, a personas naturales o jurídicas, para la atención parcial o total de los distintos canales o de los dispositivos usados en ellos, o que en desarrollo de su actividad tengan acceso a información pública clasificada o publica reservada de la entidad o de los afiliados deberá incluir acuerdos de niveles de servicio, que permitan garantizar que estos se reciban en las condiciones de tiempo, modo y lugar requeridas por la entidad, así como la seguridad, integridad, confidencialidad y disponibilidad de la información, según aplique.

19.3. Acuerdos de confidencialidad

Toda relación contractual que establezca una persona natural o jurídica con el FNA e involucre el tratamiento de información catalogada como publica clasificada o publica reservada deberá incluir un acuerdo de confidencialidad, una cláusula de cumplimiento de la política de seguridad de la información, según aplique, 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.

El acuerdo o cláusula de confidencialidad se establece entre la Entidad como contratante y el proveedor (sea una persona natural o jurídica como contratista). Si este dispone de personal o subcontratistas para la ejecución de las obligaciones contractuales, el Contratista debe garantizar que también respecto de estos cuenta con un acuerdo o cláusula de confidencialidad. Se precisa que las obligaciones respecto a la confidencialidad podrán estar incluidas dentro de las obligaciones del tercero o cláusulas específicas, o en documentos anexos al Contrato.

19.4. Protección de datos personales

Para los contratos que involucren el tratamiento de datos personales por parte de terceros y por cuenta del FNA se debe incluir una cláusula que haga referencia al cumplimiento de la Política de protección de Datos Personales del FNA y una cláusula que incluya las obligaciones y responsabilidades de cada parte en general y en caso de transferencia (nacional o internacional) de datos en los casos en que aplique, documento que debe ser entregado al Proveedor para su entendimiento y aceptación.

19.5. 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, Confidencialidad, 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.

19.6. 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

19.7. 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 Confidencialidad, 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 Control de Acceso del FNA.

• **Gestión de incidentes:** Contar 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.

19.8. Restricciones sobre el software empleado

Si el proveedor es responsable por realizar tareas que requieran la conexión de equipos de cómputo a la red corporativa de la Entidad, se deberá incluir una cláusula que establezca los requisitos de seguridad para permitir la conexión de los dispositivos a la red corporativa de la Entidad, estos requisitos deberán contener como mínimo:

• **Herramienta antimalware:** Toda máquina que se conecte a la red corporativa debe contar con una herramienta de protección de malware, que se actualice periódicamente (diariamente) y automáticamente, y realizar comprobaciones automáticas de ficheros adjuntos al correo o de aquellos que se descarguen de cualquier página web.

• **Sistema operativo:** Toda máquina que se conecte a la red corporativa del FNA debe contar con un sistema operativo debidamente licenciado, con soporte técnico por parte del fabricante y con un proceso definido e implementado para la actualización de parches de seguridad.

• **Navegador:** Toda máquina que se conecte a la red corporativa del FNA debe contar con las versiones de navegador más recientes liberadas por los fabricantes.

COPIA CONTROLADA

19.9. 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 o suministro de información catalogada como Pública Clasificada y Pública Reservada. Así mismo la que este definida en nivel Muy Alto para Integridad y Disponibilidad, a saber:

• Lista de verificación de cumplimiento de requisitos de seguridad de la información y ciberseguridad, de conformidad con el tipo de servicio prestado.
• Contar con acuerdos o cláusulas de confidencialidad de conformidad con lo descrito en el numeral 19.3Presentar la política de seguridad de la información dependiendo del servicio o producto que se está prestando al FNA.
• Presentar 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, según aplique teniendo en cuenta el tipo de servicio prestado
• Mostrar los planes de contingencia y recuperación donde muestre su capacidad de cumplir con la disponibilidad exigida en los acuerdos de niveles de servicio, si aplica.

Las empresas proveedoras cuyos servicios incluyen aspectos controlados por la legislación o regulaciones vigentes aplicables al FNA, deben asegurar y demostrar su cumplimiento.

19.10. Términos y condiciones

Cuando se contrate bajo la modalidad de outsourcing o tercerización, a personas naturales o jurídicas, para la atención parcial o total de los distintos canales o de los dispositivos usados en ellos, o que en desarrollo de su actividad tengan acceso a información pública clasificada o publica reservada de la entidad o de los afiliados deberá incluir 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, según aplique:

19.10.1. Cumplimiento de las políticas de seguridad de la información y de la política de protección de datos personales del FNA por parte del tercero, en lo que resulte aplicable de acuerdo con la naturaleza y criticidad del servicio prestado y la calidad de los datos compartidos.
19.10.2. Niveles de servicio y operación.
19.10.3. Acuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas.
19.10.4. Propiedad de la información.
19.10.5. Restricciones sobre el software empleado según sea el caso.
19.10.6. Normas de seguridad física a ser aplicadas según sea el caso.
19.10.7. Procedimientos o instructivos a seguir cuando se encuentre evidencia de alteración o manipulación de equipos o información.
19.10.8. Procedimientos o instructivos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.
19.10.9. Documentación de los controles físicos y lógicos empleados por el tercero para proteger la confidencialidad, integridad, disponibilidad de los datos y los equipos.
19.10.10. Los requisitos para la protección de la información acorde a la ley.
19.10.11. El cumplimiento explícito de la normatividad vigente y aplicable al FNA, en materia de seguridad de la información, ciberseguridad y computación en la nube, según aplique.
19.10.12. Responsabilidades de confidencialidad de la información posteriores a la terminación del contrato.
19.10.13. Responsabilidades y sanciones en caso de incumplimiento de los acuerdos respectivos.