POLÍTICA DE TRATAMIENTO DE ACTIVOS

1.1. POLÍTICA TRATAMIENTO DE INFORMACIÓN FÍSICA Y DIGITAL

1.1.1. OBJETIVO

Establecer los lineamientos generales para el tratamiento de información de la <entidad>.

1.1.2. ALCANCE

Esta política aplica para todos los funcionarios, contratistas y terceros que tengan acceso a los activos de información de la <entidad>.

1.1.3. DETALLE

El Oficial de Seguridad de la Información y/o Área de Tecnología, establecerán los controles de seguridad que permitan definir el tratamiento de información, con el fin de preservar las características de seguridad sobre los mismos. Por lo anterior, se determinarán las responsabilidades por parte de los funcionarios, contratistas y terceros mediante la celebración de contratos y/o acuerdos de confidencialidad, conforme a los lineamientos implementados por la entidad.

La <entidad> llevará a cabo un control de acceso a la información y/o activos de información contemplando aspectos físicos y lógicos, con el objetivo de garantizar la trazabilidad de las acciones realizadas por los usuarios. Dentro de los registros a generar frente a los accesos se encuentran: usuario, actividades ejecutadas, fecha, hora, lugar, intentos de acceso, accesos denegados, entre otros datos que se consideren necesarios.

Una vez se apruebe el acceso a la información, los funcionarios, contratistas y terceros no deben realizar modificaciones sobre la información sin la debida autorización, de antemano deberá salvaguardar los niveles de confidencialidad de la información a la cual tiene acceso, no vulnerar los controles de seguridad establecidos por la <entidad>, informar al Oficial de Seguridad de la Información o persona delegada acerca de las debilidades o eventos de seguridad que se identifiquen.

1.1.4. **RESPONSABILIDADES**

- Los funcionarios, contratistas y terceros de la <entidad> tienen la responsabilidad de velar por la seguridad de los activos información, asegurando que su acceso y uso sea exclusivamente para el desarrollo de las labores encomendadas, con el fin de evitar accesos no autorizados, pérdidas o uso indebido de los activos de información.

- El acceso a los activos de información será restringido teniendo en cuenta los roles y responsabilidades de los funcionarios y contratistas de la <entidad>. La autorización será otorgada por los responsables de los activos de información, previa solicitud realizada por los Jefes de Áreas o subdirectores, y conforme a lo descrito en el *Procedimiento de Gestión segura de Usuarios*. Los registros de acceso y actividades desarrolladas podrán ser auditadas para propósitos de control e investigación a los que haya lugar dentro de la naturaleza de la <entidad>, y así mismo para minimizar el riesgo de la pérdida de los niveles de seguridad de la información.

- Los funcionarios, contratistas y terceros de la <entidad> tienen como responsabilidad velar por los niveles de seguridad de la información de los

activos designados y autorizados, asegurándose que estos sólo sean utilizados para el desarrollo de las labores encomendadas. En caso de observar incidentes de seguridad, los mismos se deberán ser reportados conforme a lo establecido en el *Procedimiento Gestión de Incidentes.*

- Los accesos tanto físicos como lógicos, asignados a los funcionarios y contratistas, deberán ser desactivados o modificados una vez se termine el vínculo contractual con la <entidad>. Esto se realizará conforme a la información remitida por el Área designada por la entidad, Jefe del Área o Subdirector.

- Todos los usuarios tendrán un identificador único (ID del usuario) para su uso personal que les permita validar los accesos y verificar el buen uso de los activos de información.

- Los responsables de las áreas seguras establecerán los controles necesarios para restringir el acceso, determinando mecanismos de registro que permitan validar datos de identificación de la persona que accede a la información, el motivo del ingreso, el tiempo empleado para el desarrollo de la actividad y, asimismo, velarán por que las personas que accedan se encuentren acompañadas por un encargado durante su permanencia en ellas.

- El Responsable o Encargado del activo de información o área segura, será responsable de realizar revisiones periódicas de los derechos de acceso de los usuarios en intervalos regulares, con el fin de mantener un control eficaz de los mismos.

1.2. POLÍTICA PARA TRATAMIENTO DE ACTIVOS DE SERVICIOS

1.2.1. **OBJETIVO**

Establecer los lineamientos generales para preservar los niveles de seguridad y privacidad de los datos y activos de información accedidos por proveedores de servicios.

1.2.2. **ALCANCE**

La política aquí descrita debe ser adoptada por todos los funcionarios, contratistas y terceros de la <entidad> que tengan relación con proveedores de servicios, y que éstos accedan a activos de información propiedad de la entidad.

1.2.3. **DETALLE**

El responsable del activo de información, junto con El Oficial de Seguridad de la Información y/o Área de Tecnología, deberán llevar a cabo un análisis de riesgos para determinar los controles adecuados que se encuentren encaminados a la preservación de las características de seguridad de los activos de información que van a ser accedidos por los proveedores de servicios de la <entidad>.

Antes de brindar permisos de acceso a los proveedores, el responsable del activo de información determinará y analizar los siguientes aspectos: necesidades de acceso, tipo de acceso, nivel de clasificación de la información, finalidad de uso, controles mínimos a tener en cuenta frente al tratamiento, almacenamiento o administración de la información y los parámetros para la gestión de incidentes de seguridad de la información en

caso de presentarse. De igual manera, se verificarán los antecedentes del proveedor de acuerdo a lo establecido por el área de contratación.

Los funcionarios y/o contratistas responsables de los activos de información de la <entidad>, en ningún caso otorgarán acceso a los activos y/o áreas críticas de la entidad a los proveedores, hasta no haber realizado la formalización de la relación contractual conforme lo determina el *Manual de Contratación*, las firmas, los acuerdos de confidencialidad, y la identificación y evaluación de los riesgos de seguridad de la información.

Los acuerdos de intercambio deben, en todo caso, velar por el cumplimiento de las regulaciones legales, propiedad intelectual y protección de datos personales. Así mismo, deben especificar las consideraciones de seguridad y reserva de la información y las responsabilidades por el mal uso o divulgación de la misma.

1.2.4. **RESPONSABILIDADES**

- El responsable del activo de información, antes de otorgar los accesos a los proveedores, deberá validar que se encuentren firmados y formalizados los acuerdos de confidencialidad y el acto administrativo que determine los fines de uso, las condiciones de tratamiento de la información, así como la debida definición de los controles requeridos para preservar las características de seguridad de los activos de información.

- Los propietarios de información que se requiera intercambiar, son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma; por su parte, los custodios de esta información son responsables de implementar los controles que garanticen

el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad de acuerdo a la reglamentación vigente y los lineamientos definidos por la <entidad>.

- En caso de presentarse y/o identifique una amenaza que pueda llegar a afectar la seguridad de la información, se deberá reportar al Oficial de Seguridad de la Información y/o el Área de Tecnología a través de los canales de comunicación establecidos por la entidad.