



POLITICA DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

1. CONSIDERANDOS.....	2
2. OBJETIVO.....	3
3. DESTINATARIOS.....	3
4. ÁMBITO DE APLICACIÓN.....	4
5. ENFOQUE.....	4
6. COMPROMISO DE LA ALTA DIRECCIÓN	5
7. RENDICIÓN DE INFORMES	6
8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	6
9. OBJETIVOS ESPECÍFICOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	6
9.1. Organización de la Seguridad de la Información.....	6
9.2. Seguridad de los Recursos Humanos	7
9.3. Gestión de Activos	7
9.4. Control de acceso	7
9.5. Seguridad Física	8
9.6. Adquisición, desarrollo y mantenimiento de sistemas de información	8
9.7. Relaciones con los proveedores	9
9.8. Gestión de incidentes de seguridad de la información	9
10. DESARROLLO DE ESTA POLÍTICA.....	10
11. CONTROL.....	10
12. PROPIEDAD INTELECTUAL.....	10
13. APROBACIÓN.....	10

1. CONSIDERANDOS

- a) Que la legislación colombiana (Ley Estatutaria 1581 de 2012¹ y Ley Estatutaria 1266 de 2008², en lo que sea aplicable esta última) en materia de protección de datos personales exige a los responsables y Encargados del tratamiento de datos personales identificar e inventariar el conjunto organizado de datos o bases de datos³ que contienen información personal, sea que su tratamiento sea físico y/o automatizado.
- b) Que en el caso particular del Colegio Mano Amiga Zipaquirá, existe la obligación legal de realizar ante la Superintendencia de Industria y Comercio (SIC) como autoridad de control una declaración sobre las bases de datos que contienen información personal respecto de las cuales se realiza **cualquier** tratamiento⁴ de datos, sea físico y/o automatizado; sea que esta se realice directamente por esta organización como Responsable⁵ del Tratamiento y/o de forma indirecta a través de terceros proveedores que actúan en calidad de Encargados⁶ respecto de tales bases de datos.
- c) Que como consecuencia de la declaración obligatoria de las bases de datos con información personal tratadas a cargo del Responsable, en el Registro Nacional de Bases de Datos (RNBD) se solicita a la organización que declare el marco interno de políticas, normas y procedimientos adoptados para materializar el principio de seguridad de la información⁷, el cual es uno de los principios de mayor importancia para hacer efectivo y real el Derecho Fundamental a la Protección de Datos Personales⁸ que tiene el Titular⁹ de este tipo de dato o activo.
- d) Que esta organización en la definición del marco de cumplimiento del principio de seguridad podrá adoptar como referente las buenas prácticas de seguridad de la información contenidas en las normas estándar ISO 27001:2013, ISO 27002:2015 e ISO 27005:2018, ISO 27032:2012, NIST 800-53 rev4:2013; sin perjuicio de acudir a otras normas estándar de industria aplicables a la gestión de datos, información, conocimientos y/o gobierno de estos. Lo anterior, considerando la prevalencia de las normas legales sobre las normas estándar de industria.
- e) Que, teniendo presente el contexto anterior, esta organización entiende que los datos personales en poder de esta exigen que, una vez estos sean identificados, sean gestionados y protegidos con el fin de dar cumplimiento al régimen legal de protección de datos personales.
- f) Que el estándar de la norma ISO 27001 y demás de esta familia antes mencionadas, incorpora el dominio de cumplimiento (A.18.1)¹⁰ respecto de los requisitos de ley y

¹ Congreso de Colombia. (17 de octubre de 2012). Ley de Protección de Datos Personales. [Ley 1581 de 2012]. DO: 48.587.

² Congreso de Colombia. (31 de diciembre de 2008). Ley de Habeas Data y manejo de información financiera. [Ley 1266 de 2008]. DO: 47.219.

³ Congreso de Colombia. (17 de octubre de 2012). Artículo 3 [Título I]. Ley de Protección de Datos Personales. [Ley 1581 de 2012]. DO: 48.587.

⁴ IBID.

⁵ IBID.

⁶ IBID.

⁷ Congreso de Colombia. (17 de octubre de 2012). Artículo 4 [Título II]. Ley de Protección de Datos Personales. [Ley 1581 de 2012]. DO: 48.587.

⁸ Congreso de Colombia. (17 de octubre de 2012). Artículos 1 y 2 [Título I]. Ley de Protección de Datos Personales. [Ley 1581 de 2012]. DO: 48.587.

⁹ Congreso de Colombia. (17 de octubre de 2012). Artículo 3 [Título I]. Ley de Protección de Datos Personales. [Ley 1581 de 2012]. DO: 48.587.

¹⁰ Organización de Estándares Internacionales. (2013). Anexo A Dominio 18.1 Cumplimiento de los requisitos legales y contractuales. Sistemas de Gestión de Seguridad de la Información. [ISO 27001 de 2013].

contractuales que deben tenerse presente en la gestión de la seguridad de la información; uno de ellos es la "Privacidad y Protección de la Información Personal"¹¹.

- g) Que como expresión del compromiso de la Alta Dirección de esta organización y evidencia de la responsabilidad con la que se asume el cumplimiento del régimen de protección de datos personales se adopta esta Política; esto considerando lo dispuesto en la Guía de Responsabilidad Demostrada¹² expedida por la SIC que señala los parámetros para cumplir con el Principio de la Responsabilidad Demostrada.
- h) Que esta organización además es consciente de la importancia de identificar, proteger y gestionar otros tipos de activos de información que también son creadores de valor en la ejecución de la estrategia como son los datos, información, conocimientos y/o derechos que tenga bajo su custodia; motivo por el cual los lineamientos aquí indicados y la estrategia de seguridad de la información se extenderá no sólo a los datos personales, sino también a los demás activos de información¹³ en propiedad de esta organización y/o bajo sus custodia.
- i) Que mediante esta política se pretende fortalecer de forma más robusta e integral las prácticas de seguridad de la información existentes en la organización que han sido desplegadas de forma razonable y diligente por el Coordinador de Tecnologías de la Información.
- j) Que esta Política será desarrollada a través de normas, procedimientos y/o instructivos, los cuales serán objeto de revisión y mejoramiento permanente, acorde con los requisitos de seguridad de esta organización y dinámica de los objetivos estratégicos de la misma, en la medida que los datos, información y conocimientos tienen el potencial de crear valor para la organización y grupos de interés con los cuales se relaciona.

2. OBJETO

El objetivo o propósito de esta Política de Seguridad de la Información aplicable a los datos personales y demás activos de información es declarar que estos de acuerdo con su naturaleza son creadores de valor para la organización; razón por la cual, de acuerdo con los objetivos estratégicos y requisitos del negocio, se adoptará un esquema sistemático de gestión segura basado en riesgos con el fin de preservar los atributos de Integridad, confidencialidad y disponibilidad para fortalecer la confianza con sus grupos de interés.

3. DESTINATARIOS

Esta Política aplica a las relaciones que tiene esta organización con sus grupos de interés; a saber:

- Miembros del Consejo
- Empleados
- Proveedores
- Clientes y/o consumidores de los diferentes servicios de esta organización
- Comunidad estudiantil

¹¹ IBID.

¹² Superintendencia de Industria y Comercio. Guía para la implementación del principio de responsabilidad demostrada. Recuperado de <http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>.

¹³ Organización de Estándares Internacionales. (2013). Artículo 3 Términos y definiciones. Sistemas de Gestión de Seguridad de la Información. [ISO 27001 de 2013].

- Autoridades

4. ÁMBITO DE APLICACIÓN

Esta política de seguridad de la información será criterio rector de carácter obligatorio aplicable por los empleados en los procesos administrativos que soportan diferentes servicios que presta esta organización a los afiliados, comunidad, así como en el relacionamiento con los grupos de interés.

Igualmente será exigible en las relaciones estatutarias, contractuales y/o legales con terceros, proveedores y/o autoridades; sin perjuicio de lo aplicable a otros destinatarios de esta política.

5. ENFOQUE

Acorde a la naturaleza de esta organización el cumplimiento de los requisitos legales, estatutarios y contractuales constituye una fuente de riesgos en relación con el cumplimiento de las obligaciones de diversa naturaleza; los cuales adquieren mayor relevancia cuando un porcentaje muy alto de la operación y prestación de los servicios de la organización están soportados en Tecnologías de Información y Comunicaciones (TIC) lo que incrementa de forma importante los riesgos para la organización en relación con el logro de los objetivos estratégicos, los cuales incluyen la protección de activos de información como datos, información, conocimiento y derechos.

Esta realidad no sólo es predicable de esta organización, sino que constituye una preocupación a nivel público y privado presente también a nivel internacional; lo que ha determinado la expedición a nivel mundial de normas legales y de industria orientadas a proteger a las personas y organizaciones respecto de los riesgos cibernéticos originados en la presencia incremental de las TIC en la vida social.

Consecuencia de ello, el régimen de protección de datos personales vigente en Colombia incorpora el principio de Responsabilidad Demostrada¹⁴ mediante el cual se exige la adopción de un programa integral de protección de datos personales basado en riesgos. Este programa integral de protección de datos personales, gradualmente irá siendo extendido en esta organización a otros activos de información como datos, información, conocimiento y derechos no relacionados con datos personales.

Por tanto, el esquema de riesgos que a continuación se enuncia será considerado en la prestación de los servicios actuales de esta organización, así como en la mejora de estos y en la incorporación de los nuevos servicios, sea que involucren o no datos personales.

El enfoque de riesgos aplicable a la gestión de la seguridad de la información, que incorpora la protección de datos personales, comprende los cuatro (4) momentos fundamentales de todo sistema de gestión, como son:

Planear: Esta etapa comprende la identificación de los activos de información, entiéndase datos personales o no, información, conocimientos y/o derechos que representen un valor estratégico para la organización en relación con los objetivos estratégicos de esta y los respectivos servicios que presta a terceros, para así identificar los riesgos en relación con

¹⁴ Superintendencia de Industria y Comercio. Guía para la implementación del principio de responsabilidad demostrada. Recuperado de [https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales\(1\).pdf](https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales(1).pdf)

el cumplimiento de las obligaciones legales, estatutarias y contractuales teniendo como referencia la normatividad legal y las normas de industria o buenas prácticas aplicables según el caso. A partir de estos se establecerán los objetivos de control, controles y análisis sobre la declaración de aplicabilidad¹⁵.

Hacer: En esta etapa, previa identificación de los riesgos y definición de la declaración de aplicabilidad, se desplegarán los planes de acción orientados a prevenir, mitigar, eliminar y/o aceptar el riesgo, previo análisis y justificación de las razones por las cuales se asume este. En el plan de acción para gestionar los riesgos se determinará el responsable de la gestión, acciones a desplegar, los controles, los recursos asignados de acuerdo con su impacto y probabilidad, métricas, sin perjuicios de demás aspectos relevantes para la gestión de los riesgos vinculados.

Verificar: En esta etapa se evaluará el resultado de la gestión de la seguridad de la información respecto de los activos de información, sean datos personales o no, aplicando para ello técnicas de auditoría razonables que permitan identificar debilidades en la gestión, recomendaciones y nuevos riesgos, para así fortalecer la gestión segura de la información en la organización.

Actuar: En esta etapa a partir de los hallazgos y recomendaciones se actualizará el plan de acción para gestionar los riesgos identificados respecto de los activos de información en poder y/o custodia de esta organización.

Documentación: Es importante en términos de evaluar la debida diligencia de la Alta Dirección y demás empleados responsables¹⁶ de la gestión segura de la información la documentación y conservación de las evidencias físicas y/o electrónicas que permitan establecer que la organización ha cumplido y gestionado de forma eficaz los activos de información como datos personales o no, información, conocimientos y/o derechos.

Comunicación: Para la gestión segura de los activos de información es un elemento fundamental la comunicación interna y externa con el fin de crear, promover, mantener y fortalecer la cultura de seguridad respecto de los activos de información en poder y/o bajo custodia de la organización.

Educación y formación: El logro del objetivo de crear una cultura de seguridad de la información alrededor de los activos de información en poder y/o bajo custodia de la organización exige que la formación considere la dimensión de los riesgos que a nivel personal pueda experimentar cada empleado y/o prestador de servicios para construir al interior de la organización una cultura colectiva respecto de la protección de los datos personales y demás activos de información objeto del programa de gestión de la seguridad de la información.

6. COMPROMISO DE LA ALTA DIRECCIÓN

El régimen colombiano de protección de datos personales al dar instrucciones sobre la aplicación del Principio de Responsabilidad Demostrada establece como primer elemento para hacer realidad el Derecho Fundamental a la Protección de Datos Personales el compromiso de la Alta Dirección. Este deber legal está alineado con el deber de diligencia establecido en la normas de Código de Comercio aplicables a los administradores de la organización, el cual también está contenido en la norma de industria ISO 27001:2013 sobre gestión segura de la información la cual señala como parte de ese deber la definición de una

¹⁵ Definición de la ISO 27000 referido al documento que describe los objetivos de control, controles pertinentes y aplicables en materia de un sistema de gestión de seguridad de la información.

¹⁶ Organización de Estándares Internacionales. (2013). Anexo A Dominio 6.1 Organización Interna de la seguridad de la información. Sistemas de Gestión de Seguridad de la Información. [ISO 27001 de 2013].

política que guía la gestión segura de la información basada en riesgos, la que habrá de incorporar los requisitos de cumplimiento y articular estos con el logro de los objetivos estratégicos trazados por la organización.

7. RENDICIÓN DE INFORMES

Un componente fundamental en la seguridad de la información es mantener un proceso de comunicación efectivo que permita mantener informada a la Alta Dirección. En este orden de ideas, desde la Administración como responsable de la seguridad de la información, de forma periódica y/o excepcional, se rendirán informes respecto del estado de la seguridad de la información.

De igual forma, deberá existir una comunicación fluida desde los Departamentos que soportan los servicios que presta esta organización hacia la Administración con el fin de informar sobre las necesidades de seguridad que deben ser consideradas por la organización para su operación.

8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Dirección Administrativa de esta organización mediante esta Política declara a los grupos de interés el firme compromiso que tiene respecto del deber legal de proteger los activos de información de su propiedad y/o entregados para su custodia en virtud de una obligación legal, estatutaria y/o contractual.

Resultado del valor estratégico que tienen para esta organización los datos personales o no, información, conocimientos y derechos, se precisan los parámetros generales que deben tenerse presentes en el logro de los objetivos estratégicos en relación con la integridad, disponibilidad y confidencialidad, sin perjuicio de los otros atributos que se predicen respecto de la información.

En virtud de esta Política los procesos empresariales que soportan los servicios prestados por esta organización, cuando traten datos personales, deberán aplicar los principios relativos a la protección de datos personales señalados en la ley, jurisprudencia y/o buenas prácticas internacionales, según cada caso.

9. OBJETIVOS ESPECÍFICOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La norma ISO 27001 y las demás que hacen parte de este estándar para la gestión segura de la información definen un conjunto de objetivos específicos que contribuyen de forma armónica y sistémica a la protección de los datos, información, conocimientos y derechos ya mencionados.

En el cumplimiento de la gestión segura de la información se dará prioridad a los objetivos específicos exigidos por la normatividad legal vigente en materia de datos personales, sin que ello signifique que dejarán de atenderse aquellos otros que de forma indirecta contribuyan al objetivo general señalado en esta Política.

9.1. Organización de la Seguridad de la Información

La Alta Dirección de esta organización velará por la existencia, implementación, funcionamiento e incorporación de buenas prácticas de seguridad de la información en los procesos empresariales que soportan los servicios que presta esta organización a los afiliados y demás grupos de interés.

La Dirección Administrativa, a través de la Coordinación de Tecnologías de Información, liderará y velará por la incorporación de las buenas prácticas de seguridad de la información y para ello, con apoyo en otros procesos organizacionales, se encargará en relación con el objeto de esta política de: establecer los roles, límites y responsabilidades respecto del tratamiento¹⁷ de los activos de información; mantener contacto con las autoridades según las necesidades de la organización en esta materia; establecer los controles que protejan la información durante la operación y en los proyectos en ejecución vinculados a esta materia; velar porque los recursos informáticos a través de los cuales se gestionan activos de información y datos personales, entre otros, sean seguros.

9.2. Seguridad de los Recursos Humanos

La gestión segura de la información es una obligación que debe estar presente en todos los procesos organizacionales que soportan los servicios que se prestan a los afiliados y a la comunidad, lo cual constituye una obligación para todo empleado y/o tercero que participa en la operación de los servicios.

Corresponde al Área de Personal, en coordinación con los propietarios de los activos de información y bases de datos con datos personales a su cargo, lograr que la seguridad de la información en esta organización se gestione en los siguientes momentos: antes de la relación laboral, durante la relación laboral y después de la relación laboral.

En cualquiera de los tres momentos antes descritos, el Área de Personal definirá los lineamientos que contribuyan a la seguridad de la información y a la protección de los datos personales con el fin de mitigar riesgos y asegurar que en estos se cumplen los requisitos legales, estatutarios y contractuales vinculados al logro de los objetivos empresariales.

Es un propósito de esta organización promover y fortalecer la cultura de la seguridad respecto de los activos de información, incluidos los datos personales, considerando las necesidades de la organización y/o requerimientos de ley.

9.3. Gestión de Activos

La seguridad de los activos de información, incluidos los datos personales, requiere de la creación y mantenimiento de un inventario de estos, con el fin de gestionarlos de forma segura de acuerdo con las necesidades del negocio y/o requerimientos de ley.

Corresponde a cada propietario del activo de información con el apoyo de la Coordinación de Tecnologías de Información realizar las siguientes acciones: identificar e inventariar los activos de información, incluidos los datos personales; establecer los criterios de clasificación de estos; adoptar controles para su protección cualquiera que sea la forma de su tratamiento, considerando el ciclo de vida de los recursos en los cuales se gestionan estos.

9.4. Control de acceso

La gestión segura de la información, así como la protección de la información personal, exige que los activos de información solo sean tratados por personas autorizadas siendo

¹⁷ Congreso de Colombia. (17 de octubre de 2012). Artículo 3 [Título I]. Ley de Protección de Datos Personales. [Ley 1581 de 2012]. DO: 48.587.

para ello necesario limitar el acceso de estos a los sistemas de información, instalaciones de procesamiento y centros de gestión documental física.

Corresponderá a la organización, a través de la Coordinación de Tecnologías de Información y el respectivo propietario del activo de información, establecer los parámetros y/o directrices para crear usuarios y contraseñas; asignar derechos de acceso y tratamiento a estos; otorgar derechos de acceso privilegiado bajo el principio del mínimo necesario; adoptar mecanismos de autenticación y validación de usuarios; revisar y validar los derechos de acceso de forma periódica; y restringir y/o cancelar los accesos resultantes de la suspensión o terminación de la relación contractual, respectivamente.

El acceso a los sistemas de información se gestionará cualquiera que sea el ambiente existente para soportar los sistemas de información, sea desarrollo, pruebas, pre productivo o productivo.

El derecho de acceso a los sistemas de información cualquiera que sea su naturaleza y centros de procesamiento de datos implica una seria responsabilidad por parte del personal autorizado, por tanto, el derecho concedido es intransferible y por tanto prohibido otorgar este derecho a otra persona.

Se informa que en Colombia el acceso a los sistemas de información sin autorización y/o por fuera de lo acordado puede ser considerado un delito informático según lo dispuesto en la Ley 1273 de 2009¹⁸.

9.5. Seguridad Física

La gestión segura de la información, así como la protección de la información personal, involucra el componente físico y ambiental con el fin de prevenir el acceso no autorizado a la información tratada de forma manual, así como el daño y/o destrucción de los centros de procesamiento de los activos de información.

Corresponderá a la organización, a través de la Coordinación de Tecnologías de Información, Administración y el respectivo propietario del activo de información, establecer los parámetros y/o directrices para establecer controles de acceso, tránsito y salida de las instalaciones de la organización; adoptar controles para proteger los equipos y los activos de información en las oficinas, salones e instalaciones de la organización; definir perímetros de seguridad con el fin de proteger los activos de información sea que se trate estos de forma manual y/o automatizada; adoptar mecanismos que impidan la salida de equipos informáticos u otra naturaleza sin autorización; definir medidas que eviten el deterioro de los activos de información por factores ambientales.

Es responsabilidad de cada usuario de un activo de información aplicar las medidas de seguridad físicas adoptadas por la organización. Debe tenerse presente que los derechos de acceso a la información física se otorgan a título personal y por tanto son intransferibles.

9.6. Adquisición, desarrollo y mantenimiento de sistemas de información

La seguridad de la información y de los datos personales debe ser un requisito fundamental en los procesos de adquisición, desarrollo y mantenimiento de los sistemas

¹⁸ Congreso de Colombia. (05 de enero de 2009). Ley de protección de la información y de los datos y modificación del código penal. [Ley 1273 de 2009]. DO: 47.223

de información, en los cuales debe garantizarse la integridad, disponibilidad y confidencialidad de los activos de información durante todo el ciclo de vida de estos; sea que la gestión la realice directamente la organización y/o se contrate con un tercero proveedor.

Corresponderá a la organización, a través de la Coordinación de Tecnologías de Información, el Área de Compras y el respectivo o futuro propietario del activo de información, señalar parámetros para establecer en cada caso los requisitos de seguridad y protección de datos personales que deben estar presentes en el sistema de información; incorporar mecanismos que validen y verifiquen los datos de entrada, salida y procesamiento completo de las transacciones; adoptar prácticas seguras de desarrollo de sistemas de información; implementar prácticas seguras de control de cambios; definir esquemas de pruebas; definir los mecanismos de monitoreo con el fin de que los accesos sean autorizados y/o detectar irregularidades; y diseñar estrategias de salida en producción que no comprometan la operación de los servicios de la organización.

Es responsabilidad de todo líder de proceso empresarial y/o servicio involucrado en la adquisición, desarrollo y mantenimiento de sistemas de información definir al inicio del proyecto los requisitos que permitan garantizar la seguridad de los activos de información y datos personales tratados en el respectivo sistema de información.

Es indispensable que toda adquisición, desarrollo y/o mantenimiento de un sistema de información incluya las redes, incorpore como requisito la seguridad de los activos de información y protección de datos personales en cualquier de los momentos del proyecto, independiente de que este lo ejecute directamente la organización y/o se contrate con un tercero.

No son aceptables sistemas de información que adolezcan de funcionalidades que omitan la seguridad de los activos mencionados, incluidos los datos personales.

9.7. Relaciones con los proveedores

La seguridad de la información es un deber que involucra a los terceros proveedores que, en razón de las relaciones precontractuales, contractuales o postcontractuales acceden y/o realizan cualquier tratamiento respecto de los activos de información, incluidos los datos personales, que están en poder y/o bajo la custodia de esta organización.

Corresponde a esta organización adoptar directrices internas en materia de seguridad de la información las cuales fortalecerán los criterios a tener presentes en la selección y contratación de proveedores que deban acceder y/o tratar activos de información, incluidos los datos personales.

9.8. Gestión de incidentes de seguridad de la información

La seguridad de la información y de los datos personales imponen a la organización la obligación de gestionar de forma adecuada los incidentes de seguridad que comprometan algún activo de información; siendo obligación reportar ante la SIC aquellos que hayan comprometido cualquier tipo de dato personal.

Corresponde a la Coordinación de Tecnologías de Información en relación con la gestión de los incidentes de seguridad de la información adoptar el procedimiento para la gestión de estos y consecuente respuesta, así como desplegar un plan de acción que de forma periódica evalúe las debilidades de la seguridad de la información a nivel físico e informático; clasificar y analizar los eventos de seguridad para definir si han alcanzado el nivel de incidentes; gestionar el conocimiento a partir de los incidentes para adoptar

controles que mejoren la seguridad de la información y fortalezcan las competencias para responder a los incidentes de seguridad de la información, sea que incluyan datos personales o no.

Es responsabilidad de la Coordinación de Tecnologías de Información como responsable de la Protección de Datos Personales gestionar de forma adecuada todo incidente de seguridad de la información que comprometa datos personales. El Informe del incidente de seguridad, realizado a partir del procedimiento de atención a este, será presentado a la Alta Dirección con el fin de informar sobre la situación, para efectos del reporte que debe realizarse a la Sic como autoridad de control en el término establecido en la ley.

La gestión del incidente de seguridad respecto de un activo de información y/o datos personales debe ser pactado como obligación de los proveedores involucrados de forma directa o indirecta en el incidente de seguridad; tal como lo exige el régimen de Protección de Datos vigente en Colombia.

Es obligación de todo destinatario de esta norma informar sobre la sospecha de una situación que pueda comprometer la seguridad de un activo de información, incluidos los datos personales, reporte que se realizará a la Coordinación de Tecnologías de Información conforme el procedimiento adoptado para este fin.

10. DESARROLLO DE ESTA POLÍTICA

Esta Política se desarrolla a través de un conjunto de normas, procedimientos, guías, formatos y/o Instrumentos normativos adoptados por esta organización, a través de la Administración Coordinación de Tecnologías de Información.

11. CONTROL

El responsable de este documento es la Administración a quien corresponde revisarlo al menos una vez al año y realizar una actualización si lo considera necesario o realizar esta cuando surja un cambio importante; caso en el cual deberá ser aprobado por la Alta Dirección y comunicarlo a los destinatarios y/o partes interesadas de este documento.

12. PROPIEDAD INTELECTUAL

Este documento es solo para uso empresarial, pues tiene derechos reservados de autor, por tanto, está prohibida su copia, reproducción total o parcial, modificación y ejercicio de cualquier derecho patrimonial de autor no autorizado de forma expresa por sus creadores.

13. APROBACIÓN

Esta Política de Seguridad de la Información ha sido aprobada DIA/MES/AÑO por la Dirección del Colegio Mano Amiga Zipaquirá.