POLÍTICA DE SEGURIDAD PARA EL TRATAMIENTO DE LA INFORMACIÓN

ASOCIACIÓN PARA LA ENSEÑANZA ASPAEN

23 de enero de 2025

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
ASOCIACIÓN PARA LA ENSEÑANZA - ASPAEN

Contenido

1. INTRODUCCIÓN

La **ASOCIACIÓN PARA LA ENSEÑANZA - ASPAEN** (en adelante, **ASPAEN**) ha implementado una Política de Seguridad de la Información, en atención a la identificación de las responsabilidades y objetivos que debe trazar una organización como Responsable de la información y del Tratamiento de Tratamiento de Datos Personales, con la finalidad de suministrar una protección adecuada a los activos de la información y de reducir los riesgos que puedan conllevar a la divulgación, modificación, destrucción o utilización indebida de estos.

La presente Política de Seguridad de la Información, está conformada por estándares, procedimientos y herramientas de verificación y control, con el propósito de orientar y robustecer las medidas humanas, técnicas y administrativas que permitan a **ASPAEN,** administrar la información bajo el Principio de Seguridad y los criterios orientadores en la identificación y gestión de los riesgos de seguridad y privacidad.

2. OBJETO

Este documento establece los lineamientos para velar por el cumplimiento de los principios de confidencialidad, integridad, disponibilidad, legalidad, finalidad, libertad, veracidad y/o calidad, seguridad, transparencia, acceso y circulación de la información[1] en el Tratamiento de los Datos Personales y la gestión de la información que lleva a cabo **ASPAEN**, de tal manera que permita a la organización mantener y robustecer la postura de seguridad de la información.

3. ALCANCE

Los presentes lineamientos aplican a todos los colaboradores, proveedores y/o terceros, que tengan acceso a los activos de la información de **ASPAEN**.

4. MARCO NORMATIVO

MARCO NORMATIVO APLICABLE	
Disposición Legal	**Descripción**
Constitución Política de Colombia	**Artículo 15**: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacer los respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas".
Ley Estatutaria 1581 de 2012	Se dictan disposiciones para la Protección de los Datos Personales. La norma tiene por objeto "(…) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías

[1] Ley 1581 de 2012, artículo 4°.

MARCO NORMATIVO APLICABLE	
Disposición Legal	**Descripción**
	constitucionales a que se refiere el artículo 15 de la Constitución Política (…)"[2].
Decreto 1377 de 2013	Por medio del cual se reglamenta parcialmente la Ley 1581 de 2012 que constituye el marco general de la protección de los datos personales en Colombia.
Decreto 1074 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos.
Decreto 338 de 2022	Por el cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las Instancias de Gobernanza de Seguridad Digital.
Ley 1273 de 2009	Modifica el Código Penal y se crea un nuevo bien jurídico tutelado que se denomina "protección de la información y de los datos".
Ley Estatutaria 1266 de 2008	Se dictan disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de Datos Personales, en especial la financiera, crediticia, comercial, de servicios y proveniente de terceros países.
Ley 527 de 1999 (Acceso y Uso de Mensajes de Datos)	Se define y se reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
CONPES 3701 de 2011	Se dictan lineamientos de Política Nacional para Ciberseguridad y Ciberdefensa.
CONPES 3854 de 2016	Dicta disposiciones sobre la Política Nacional de Seguridad Digital.

Es preciso resaltar que, para la elaboración de la presente política, se incluyeron aspectos de regulación aplicable al sector público[3]. Si bien **ASPAEN**, en principio, no es sujeto obligado de dichas normas, se integran y se toman como referencia por las buenas prácticas que son adoptadas por **ASPAEN** para garantizar la seguridad de la información durante todo el Tratamiento de los Datos Personales.

5. GLOSARIO

Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tienen un valor para la organización[4].

Activo de la información: Recurso o elemento que contiene información con valor para la organización debido a su utilización en algún proceso, o que tiene relación directa o indirecta con las actividades de la empresa: software hardware, personas (roles), físicos (instalaciones, área de almacenamiento de expedientes, centros de procesamiento de datos), intangibles (imagen y reputación)[5].

[2] Ley 1581 de 2012, artículo 1°.
[3] Tales como las normas CONPES, el Decreto 338 de 2022, Ley 1712 de 2014, Guías del Ministerio de Tecnologías y Comunicaciones y Circulares, entre otras.
[4] ISO 27000
[5] ISO 27001

Amenazas: "Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización"[6].

Amenaza Informática: "Toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio"[7].

Antivirus: Es considerada como una categoría de software de seguridad que busca proteger un equipo de virus, normalmente, a través de la detección en tiempo real y también mediante análisis del sistema que pone en cuarentena y elimina los virus[8].

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar su nivel de riesgo[9].

Anonimización del Dato: Eliminar o sustituir datos para evitar la identificación de personas y preservar la confidencialidad de la información[10].

Autenticación: Mecanismo técnico que permite garantizar que una persona o entidad es la correcta[11].

Back Up: Hace referencia a una copia de respaldo de la información.

Buzón: espacio de almacenamiento de información reservado en un servidor de correo electrónico con fines de almacenar correos, contactos, calendario, entre otros.

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética[12].

Confidencialidad: Propiedad que ostenta la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados[13].

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[14].

Integridad: La propiedad de salvaguardar la exactitud y completitud de la información.[15]

Control informático: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. El control también es utilizado como sinónimo de salvaguarda o

[6] Guía para la Implementación de Seguridad de la Información en una MIPYME – Ministerio de las Tecnologías y Comunicaciones. https://gobiernodigital.mintic.gov.co/692/articles-150522_Guia_Seguridad_informacion_Mypimes.pdf
[7] Guía para la Implementación de Seguridad de la Información en una MIPYME – Ministerio de las Tecnologías y Comunicaciones. https://gobiernodigital.mintic.gov.co/692/articles-150522_Guia_Seguridad_informacion_Mypimes.pdf
[8] Guía para la Implementación de Seguridad de la Información en una MIPYME – Ministerio de las Tecnologías y Comunicaciones. https://gobiernodigital.mintic.gov.co/692/articles-150522_Guia_Seguridad_informacion_Mypimes.pdf
[9] ISO 27000
[10] https://www1.funcionpublica.gov.co/documents/418537/36701283/politica-de-seguridad-de-la-informacion.pdf.pdf/325019e5-a92f-0b44-3676-2356bd71240c?t=1586355315672
[11] ISO 27001
[12] CONPES 3701
[13] NTC-ISO/IEC 27001
[14] NTC-ISO/IEC 27001
[15] NTC-ISO/IEC 27001

contramedida, es una medida que modifica el riesgo reduciendo la probabilidad o impacto del evento[16].

Contraseña: "Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales." "Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña"[17].

Datos biométricos: Parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona, o una parte de ella, interacciona con el sistema (ej. huella digital o voz). Representan datos sensibles de la persona[18].

Dato Personal: "Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables."[19]

Datos Sensibles: Son aquellos Datos que "(…) afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos."[20]

Dato Privado: "Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular."[21]

Datos Semiprivados: Son aquellos Datos "que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial (…)"[22]

Datos Públicos: Son datos calificados como tal por mandato legal o constitucional. "Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas."[23]

Evento de seguridad de la información: Ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.[24]

Gestión de incidentes de seguridad de la información: Proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.[25]

---

[16] ISO 27000
[17] Guía para la Implementación de Seguridad de la Información en una MIPYME – Ministerio de las Tecnologías y Comunicaciones. https://gobiernodigital.mintic.gov.co/692/articles-150522_Guia_Seguridad_informacion_Mypimes.pdf
[18] https://www.sic.gov.co/content/los-datos-personales-y-la-propiedad-industrial#:~:text=%C2%BFQu%C3%A9%20son%20los%20datos%20biom%C3%A9tricos.datos%20sensibles%20de%20la%20persona
[19] Ley 1581 de 2012, artículo 3°.
[20] Decreto 1377 de 2013, artículo 3°.
[21] Ley 1266 de 2008, artículo 3°.
[22] Ley 1266 de 2008, artículo 3°.
[23] Ley 1266 de 2008, artículo 3°.
[24] ISO 27001:2022
[25] ISO 27001:2022

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, comprende la identificación, evaluación y el tratamiento de riesgos.[26]

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones.[27]

Impacto: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.[28]

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.[29]

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.[30]

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del Sistema de gestión de seguridad de la información, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.[31]

Plan de continuidad del negocio: Plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.[32]

Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.[33]

Responsable de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado encargado de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados, quien puede designar custodios del activo de información y autorizar a los usuarios para el acceso al activo de información.

Responsable del Tratamiento: Aquella persona natural o jurídica, pública o privada que por sí misma o en asocio con otros decida sobre la base de datos y/o el Tratamiento de los Datos.[34]

Titular de la información: "Persona natural cuyos datos personales sean objeto de Tratamiento".[35]

[26] NTC-ISO/IEC 27001
[27] ISO Guía 73:2002
[28] ISO 27000
[29] ISO 27000
[30] NTC-ISO/IEC 27001
[31] ISO 27000
[32] ISO 27000
[33] ISO 27000
[34] Ley 1581 de 2012, artículo 3°.
[35] Ley 1581 de 2012, artículo 3°.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.[36]

Vulnerabilidad: Es un estado viciado en un sistema informático que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas.[37]

6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

ASPAEN, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido a proteger, preservar y administrar la confidencialidad, integridad, disponibilidad y no repudio de la información, mediante una gestión integral de riesgos, implementación de controles físicos y digitales, con la finalidad de prevenir incidentes, y dando cumplimiento a los requerimientos legales.

Por tal motivo, **ASPAEN** ha definido e implementado una Política de Seguridad y Privacidad de la Información, teniendo en cuenta los siguientes aspectos:

1. Proteger los activos de la información, mediante políticas, procedimientos e instructivos en materia de seguridad de la información, teniendo en cuenta el Ciclo de Vida Útil del Dato.
2. Aplicar controles de acceso a la información creada, procesada, transmitida o resguardada por los procesos propios de las actividades de **ASPAEN**, con la finalidad de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta, teniendo en cuenta la clasificación de la información a la cual se le hace Tratamiento.
3. Mitigar el riesgo de vulnerabilidad en la seguridad de la información, en la ejecución de los procesos y actividades propias de **ASPAEN**, a través de una adecuada gestión de eventos de seguridad y riesgos asociados al Tratamiento de Datos Personales y gestión de la información.
4. Cumplir con los principios (Disponibilidad, Integridad y Confidencialidad) de seguridad de la información.
5. Fortalecer la cultura de seguridad de la información al interior de la organización.
6. Verificar de manera periódica el cumplimiento de las políticas de seguridad de la información.
7. Cumplir las obligaciones legales, regulatorias y contractuales establecidas.

7. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

7.1. ROLES EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

En atención a la estructura organizacional de **ASPAEN,** la persona encargada de efectuar la verificación del cumplimiento y respectivo seguimiento de las medidas establecidas en la Política de Seguridad y Privacidad de la Información será el Oficial de Seguridad de la Información.

[36] ISO 27000
[37] Guía para la Implementación de Seguridad de la Información en una MIPYME – Ministerio de las Tecnologías y Comunicaciones. https://gobiernodigital.mintic.gov.co/692/articles-150522_Guia_Seguridad_informacion_Mypimes.pdf

En cabeza del Oficial de Seguridad de la Información recaen, principalmente, las siguientes funciones:

1. El desarrollo, la implementación y la actualización de las políticas y estrategias de seguridad partiendo de las buenas prácticas a nivel nacional e internacional. En este orden de ideas, se debe supervisar que las medidas de seguridad implementadas sean cumplidas por los colaboradores, proveedores y/o terceros.
2. Identifica, evalúa y mitiga los riesgos que estén relacionados con la información y la tecnología que se maneja al interior de la organización.
3. La implementación de programas de capacitación para empleados, estudiantes y colaboradores encaminados a promover una cultura de seguridad.
4. Monitorear y evaluar el sistema de seguridad para garantizar el cumplimiento de la normativa vigente.

7.2. GESTIÓN DE ACTIVOS

7.2.1. Responsabilidad frente a los activos de la información

1. Propender por la seguridad y la calidad de la información, siguiendo criterios de confidencialidad, integridad, disponibilidad, efectividad, eficiencia, confiabilidad y cumplimiento, en calidad de colaboradores, proveedores y/o terceros con quienes **ASPAEN** tenga relación al ejecutar sus actividades.
2. Cumplir con las políticas y los controles de seguridad de la información definidos, para garantizar la preservación de la confidencialidad, integridad, disponibilidad de los activos de la información de la organización, y recuperación de la información.
3. Está prohibido hacer modificaciones a los activos de la información, sin contar con autorización para ello.
4. Está prohibido hacer uso de los activos de la información de **ASPAEN**, para fines diferentes al cumplimiento de las actividades propias de la organización.
5. Hacer el inventario de todos los activos de la información, los cuales deben estar asignados a un responsable.
6. Actualizar de manera periódica todos los activos de la información, con los lineamientos relacionados con las restricciones de acceso a la misma.
7. Ser el responsable del uso y protección de los activos de la información, en calidad de encargado de esta, mientras se encuentre en su custodia física o digital.
8. Informar cualquier incidente de seguridad que pueda presentarse, tales como: uso indebido, alteración y/o divulgación no autorizada.

7.2.2. Identificación de los activos

Los activos de la información con que cuenta **ASPAEN** está conformada por: la información relativa a la constitución y composición de la organización y siete (7) bases de datos denominadas de la siguiente manera: “Empleados y exempleados”, “Alumnos y Ex Alumnos”, “Padres de Familia de Alumnos y Ex Alumnos”, “Proveedores”, “Deudores”, “Donantes” y “Órganos de Gobierno”[38].

7.2.3. Etiquetado de la Información

[38] Información recopilada del Registro Nacional de Bases de Datos de la Superintendencia de Industria y Comercio.

Con la finalidad de identificar la naturaleza y los tipos de Datos Personales y en general, información, respecto de la cual se lleva a cabo Tratamiento; se debe tener en cuenta la siguiente clasificación:

1. **Información Pública:** Los Datos Públicos son aquellos que son de interés general. Entre estos Datos se encuentra los relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva[39].

2. **Información Privada:** Los Datos Privados son aquellos que por su naturaleza íntima o reservada sólo es relevante para el Titular de la información tales como la dirección de residencia y teléfono de contacto[40]. En relación con los activos de información de esta categoría, es preciso indicar que, su característica radica en la pertenencia una órbita propia, particular y privado o semiprivado de una persona natural o jurídica.

3. **Información Semi Privada:** Los Datos Semi Privados no ostentan de naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su Titular sino a cierto sector o grupo de personas (como lo puede ser la historia crediticia del Titular)[41].

4. **Información Sensible o Reservada:** Se entiende por Datos Sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos[42]. En relación a los activos de información reservados, son aquellos que ante una indebida divulgación podría representar un daño a intereses generales, públicos o propios de la organización.

El responsable de verificar el entendimiento y la debida clasificación de la información será del Oficial de Seguridad de la Información de **ASPAEN** junto a su equipo de trabajo.

7.2.4. Disposición de los activos

Con el objetivo de establecer reglas para el uso aceptable de los activos de la información identificados y la infraestructura destinada al procesamiento de esta, se documentarán las restricciones necesarias para la gestión de la información, de acuerdo con los requisitos de protección determinados a partir de la clasificación de la información.

Se registrarán los colaboradores autorizados de **ASPAEN** que intervienen en los procesos que gestionan y procesan los activos de la información. Es decir, además de identificar los activos de la información, se identificarán las personas responsables del uso y/o gestión de la información.

[39] Decreto 1377, artículo 3°.
[40] Sobre la protección de datos personales – Superintendencia de Industria y Comercio. https://www.sic.gov.co/content/sobre-la-protecci%C3%B3n-de-datos-personales
[41] Sobre la protección de datos personales – Superintendencia de Industria y Comercio. https://www.sic.gov.co/content/sobre-la-protecci%C3%B3n-de-datos-personales
[42] Decreto 1377 de 2013, artículo 3°.

Los lineamientos y procedimientos de operación de TI en **ASPAEN** establecerán las acciones en el manejo de cualquier medio móvil y reusable que vaya a ser transportado o dado de baja de la organización. Una vez removidos los medios, se tomarán las medidas para garantizar que la información no sea recuperable, estas actividades deberán ser registradas, documentadas e informadas a los responsables de los procesos de respaldo y recuperación de información.

El transporte de medios con información misional deberá ser a través de proveedores de servicio especializado debidamente certificados. Las autorizaciones previas de traslado o eliminación de medios deberán contar con el registro y la disponibilidad para su posterior consulta. Los formatos utilizados para el almacenamiento de la información, de acuerdo con su clasificación y valoración de riesgo, deberán ser estándares vigentes en el mercado tanto en el cifrado como en la locación de la información, esto con el fin de facilitar su recuperación.

Por lo tanto, el seguimiento a los ejercicios periódicos de recuperación de copias de seguridad evaluará la efectividad de la restauración y la vigencia tecnológica a la infraestructura de "*BackUp*".

7.3. POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN

7.3.1. Objetivo

Establecer las definiciones de acceso a los usuarios autorizados a los sistemas, aplicaciones y demás recursos tecnológicos, ejerciendo, la asignación, modificación, revocación y gestión de permisos bajo los siguientes lineamientos:

1. Mínimo privilegio.
2. La estricta necesidad de cumplir con las funciones asignadas.
3. Control dual establecido en los flujos de roles y perfiles.
4. La coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes.
5. Los requerimientos de seguridad de cada una de las aplicaciones.
6. Toda la información relacionada con las aplicaciones.
7. La legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
8. Los perfiles de acceso de usuarios base, comunes a cada categoría de puestos de trabajo.
9. La administración de los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.
10. La revisión periódica de los derechos de acceso para garantizar que sigan siendo los apropiados.

7.3.2. Herramientas utilizadas al interior de ASPAEN

Al interior de **ASPAEN** se utilizan, principalmente, las herramientas denominadas *Azure Entra ID* y *Microsoft Intune* para garantizar un acceso controlado a la información, de acuerdo con las responsabilidades que ostenta cada uno de los colaboradores.

Las plataformas mencionadas previamente son utilizadas de la siguiente manera:

1. **Azure Entra ID:** Se da la configuración de los roles a través de la sección denominada *"Roles and Administrators*" para dar una asignación precisa. Con esta herramienta se restringe el acceso según las condiciones de ubicación, dispositivo y riesgo.

   Al interior de la herramienta se pueden asignar los siguientes roles:
   1. *Global Administrator:* Se limita a un máximo de tres usuarios para garantizar la seguridad.
   2. *User Administrator:* Encargado de gestionar usuarios y grupos.
   3. *Device Administrator:* Responsable de la gestión de los dispositivos.
   4. *Application Administrator*: Acceso para gestionar las aplicaciones corporativas.

2. **Microsoft Intune:** Es utilizada para la creación de políticas de cumplimiento para garantizar que los dispositivos utilizados sean seguros. En esta aplicación se utilizan los siguientes roles:

   1. *Intune Administrator:* Gestiona las configuraciones globales y directivas de los dispositivos.
   2. *Policy and Profile Manager*: Define y supervisa las políticas de cumplimiento.
   3. *Helpdesk Operator:* Acceso para resolver incidentes relacionados con los dispositivos y los usuarios.

7.3.3. Asignación de roles, permisos y/o asignación de contraseñas

Los permisos concretarán qué acciones pueden realizar sobre la información (creación, lectura, borrado, modificación, copia, ejecución, etc.). Como norma general, siempre se otorgará el mínimo privilegio en el establecimiento de los permisos. Además, la asignación de roles se realizará a partir de la función del cargo y las responsabilidades que tenga el empelado.

Se identificarán los niveles de acceso necesarios para cada cargo dentro **ASPAEN**. Estos se agruparán en las siguientes categorías:

1. **Administradores:** Acceso completo a sistemas críticos, configuraciones y supervisión.
2. **Supervisores/Responsables de área:** Acceso a los recursos y datos necesarios para liderar sus equipos.
3. **Colaboradores Operativos:** Acceso limitado a las herramientas y recursos requeridos para su trabajo diario.
4. **Terceros/Contratistas**: Acceso restringido y temporal a recursos específicos según contratos o acuerdos.

Por otro lado, la asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el siguiente flujo:

1. Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto.
2. Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisionales, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.

3. Generar contraseñas provisionales para iniciar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.

7.3.4. Creación/ modificación/ borrado de cuentas de usuario

Para permitir el acceso a los sistemas de información de **ASPAEN** deberá seguirse el procedimiento que permita gestionar la creación/modificación/borrado de las cuentas de acceso de los usuarios indicando quién debe autorizarlo. Detallar los datos identificadores de las mismas, las acciones que se permiten y dotándolas de las credenciales de acceso correspondientes que deberán ser entregadas de forma confidencial a sus dueños. Se incluirán, asimismo, parámetros tales como la caducidad de las contraseñas y los procedimientos de bloqueo oportunos. Se debe informar al usuario de estos requisitos al entregarle las credenciales.

7.3.5. Cuentas privilegiadas

El responsable de la Información limitará y controlará la asignación y uso de privilegios. Los sistemas multiusuario que requieren protección contra accesos no autorizados deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.

Se deben tener en cuenta los siguientes pasos:

1. Identificar los privilegios asociados a cada activo que requiera el acceso de usuarios, por ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
2. Asignar los privilegios a usuarios sobre la base de la necesidad de uso y evento por evento.
3. Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
4. Establecer un periodo de vigencia para el mantenimiento de los privilegios, luego del cual los mismos serán revocados. No existirán usuarios sin fecha de vigencia.
5. Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

7.3.6. Mecanismos de autenticación

Se implementan mecanismos de autenticación adecuados para permitir el acceso a la información de la organización. Teniendo en cuenta aspectos como:

1. Utilización de mecanismos de autenticación internos o basados en servicios de autenticación de terceros.
2. Factores de los mecanismos de autenticación: Por ejemplo, a través de técnicas biométricas, contraseñas y/o tokens criptográficos.

7.3.7. Registro de eventos

Se deberán establecer los mecanismos necesarios para registrar los eventos relevantes garantizando su conservación y acceso autorizado en el manejo de la información de la organización.

Asimismo, se registrará convenientemente quién accede a la información, cuándo, cómo y con qué finalidad.

7.3.8. Revisión de permisos

Los dueños de los activos de la información que corresponde a los servicios de aplicación establecerán los requerimientos periódicos para la evaluación de los permisos, incluyendo los usuarios privilegiados.
Los roles y permisos serán revisados de manera periódica (trimestralmente) por el área de seguridad para identificar asignaciones innecesarias o riesgosas.

7.3.9. Revocación de permisos

En cumplimiento de los procedimientos de gestión de usuarios a partir de las solicitudes de los dueños de los activos, se tomarán las acciones suficientes y necesarias para revocar los privilegios, permisos y accesos de cualquier usuario, qué por motivos de traslados o desvinculación requiera dicha revocación. Se deberán ofrecer los mecanismos técnicos para su cumplimiento registro y seguimiento.

Ante cualquier acceso indebido, también serán revocados los permisos de inmediato y se realizará el respectivo reporte del suceso.

7.4. CONTROLES ESPECÍFICOS PARA EL ACCESO A DATOS SENSIBLES

Al interior de **ASPAEN**, se cuenta con políticas claras, definidas y específicas para el acceso a la información que garantizan la protección de los Datos Sensibles y la seguridad de los sistemas.

Las Políticas están diseñadas para limitar y controlar el acceso a la información. Para lo anterior, se tiene en cuenta el etiquetado de la información, específicamente, de los Datos Sensibles.

En función de esto, se hace uso de diferentes herramientas tales como *Azure Entra ID*, *Microsoft Intune* y *Fortinet* que permiten cumplir con las siguientes actividades:

1. Gestionar y restringir el acceso a los recursos en función de condiciones específicas.
2. Autenticar y autorizar a los usuarios de manera segura mediante el uso de diferentes tecnologías.
3. Aplicación de actualizaciones automáticas y de políticas de cifrado para proteger la información sensible.Gestionar y restringir el acceso a los recursos en función de condiciones específicas.
4. Autenticar y autorizar a los usuarios de manera segura mediante el uso de diferentes tecnologías.
5. Aplicación de actualizaciones automáticas y de políticas de cifrado para proteger la información sensible.
6. Controlar el acceso y uso de aplicaciones corporativas con la finalidad asegurar un entorno seguro.

7. Administración del Firewall.

7.5. CONTROLES CONTRA SOFTWARE MALICIOSO

ASPAEN establece los controles de detección y prevención para la protección contra software malicioso, estableciendo y ejecutando los procedimientos adecuados de concientización de usuarios en materia de seguridad y controles de acceso al sistema.

7.5.1. Herramientas para los controles contra software malicioso utilizados

ASPAEN cuenta con robustos controles para la detección y prevención de software malicioso. Principalmente, se cuenta con el apoyo de la herramienta *Microsoft Defender* a través de la cual se protegen los activos digitales de manera integral.

Dicha herramienta apoya en los siguientes controles:

1. Protección contra malware y virus a través de la identificación y eliminación de diferentes amenazas.
2. Supervisión y respuesta a incidentes por medio del monitoreo continuo de dispositivos y redes para identificar intentos de acceso no autorizado o actividad maliciosa. También, se da la generación de alertas detalladas y acciones automáticas para contener y mitigar la amenaza en tiempo real.
3. Garantiza la seguridad de todos los dispositivos que son utilizadnos al interior de **ASPAEN.**
4. Proporciona herramientas avanzadas para investigar incidentes de seguridad y rastrear la causa raíz.
5. Detecta y mitiga amenazas avanzadas, incluyendo ataques dirigidos y ransomware, mediante inteligencia proactiva y de análisis comportamental.

7.6. ESCRITORIO LIMPIO

Esta política tiene por objetivo salvaguardar los activos de información asociados a los puestos de trabajo y equipos de cómputo a través de las acciones de mantener un puesto de trabajo limpio y datos de procesamiento de información no expuestos, para reducir los riesgos de acceso no autorizado, fuga o daño de la información durante y después de la jornada laboral.

Se debe configurar en las estaciones de trabajo el bloqueo de sesión, el cual debe activarse automáticamente máximo después de ciento ochenta segundos o tres minutos de inactividad y será necesario para ingresar a la sesión, escribir la contraseña del usuario.

Siempre que un usuario se ausente de su computador de trabajo, debe realizar el bloqueo de la sesión oprimiendo la tecla de **Windows + la tecla L** para evitar riesgos de acceso no autorizado.

No se deben escribir las contraseñas en notas adhesivas en el escritorio o cualquier otro medio visual, ni mantenerlas a la vista de las demás personas.

Cuando se envié documentos a imprimir, el documento impreso debe retirarse inmediatamente de la impresora.

Al finalizar la jornada de trabajo se debe guardar en un lugar seguro bajo llave, los documentos y medios que contengan información necesaria para el cumplimiento de las actividades de **ASPAEN.**

7.7. ACCESO REMOTO

Los usuarios podrán acceder en forma remota a los activos de información a través de una plataforma de conexiones de VPN. Para el acceso deberá solicitarse la correspondiente autorización. En cualquier situación, dicho acceso será gestionado por el personal asignado para ello y solo podrá tener por finalidad dar soporte a equipos tecnológicos o sistemas de información, revisar errores de funcionamiento o prestar servicios de seguridad y/o monitoreo.

Se debe mantener un registro de los accesos que se han realizado a través de la VPN para efectos de trazabilidad y posterior revisión en caso de ser requerido.

El acceso por VPN debe estar asociado a la gestión de usuarios y seguir los mismos lineamientos de creación, modificación, revocación, cambio y monitoreo.

7.8. NO REPUDIO

Esta Política de Seguridad y Privacidad comprende la capacidad de no repudio, con el fin de que los usuarios eviten haber realizado alguna acción. La Política deberá incluir mínimo los siguientes aspectos:

1. **Trazabilidad:** La Política hará que, por medio de la trazabilidad de las acciones, se haga seguimiento a la creación, origen, recepción, entrega de información y otros.
2. **Retención**: La Política debe incluir el periodo de retención o almacenamiento de las acciones realizadas por los usuarios, el cual deberá ser informado a los funcionarios, contratistas y/o terceros.
3. **Auditoría**: La Política incluirá la realización de auditorías continuas, como procedimiento para asegurarse que las partes implicadas nieguen haber realizado una acción.
4. **Intercambio electrónico de información:** La Política incluirá en los casos que aplique, que los servicios de intercambio electrónico de información son garantía de no repudio.

7.9. LA POLÍTICA DE PRIVACIDAD Y CONFIDENCIALIDAD

7.9.1. Objetivo

Describir las políticas de Tratamiento y Protección de Datos Personales que deben aplicarse, conforme a la normatividad vigente.

7.9.2. Principios del Tratamiento de Datos Personales[43]

[43] Ley Estatutaria 1581 de 2012. “Régimen General de Protección de Datos Personales”.

1. **Principio de legalidad:** El Tratamiento de Datos Personales debe estar sujeto a lo establecido en la normatividad vigente.
2. **Principio de finalidad:** La finalidad del Tratamiento de Datos Personales debe ser informada al Titular.

3. **Principio de libertad:** El Tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del Titular de los Datos Personales.

4. **Principio de veracidad o calidad**: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.

5. **Principio de transparencia:** Garantizar al Titular de los Datos el derecho a obtener información que le concierna del encargado del Tratamiento.

6. **Principio de acceso y circulación restringida:** El Tratamiento sólo podrá llevarse a cabo por personas autorizadas por el Titular o por personas previstas en la normatividad vigente.

7. **Principio de seguridad:** La información sujeta a Tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

8. **Principio de confidencialidad**: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información.

La Política de Tratamiento de Datos Personales de **ASPAEN** puede ser consultada a través de la siguiente la página web: https://aspaen.edu.co/wp-content/uploads/Politica-de-Tratamiento-de-Datos-ASPAEN.pdf

7.9.3. Acuerdo de Confidencialidad

Con la finalidad de preservar la confidencialidad y privacidad de la información que se maneja en **ASPAEN**, se hará uso del acuerdo de confidencialidad implementado con colaboradores, contratistas y/o terceras personas, en aquellos eventos en que la información que se esté tratando lo amerite.

7.10. POLÍTICA DE DISPONIBILIDAD DE LA INFORMACIÓN

7.10.1. Planes de recuperación

Con el objetivo de garantizar la continuidad de los servicios ante posibles eventos no deseados que interrumpan la operación de los procesos de **ASPAEN**, se debe identificar los eventos que puedan ocasionar interrupciones en los procesos operaciones de TI, por ejemplo, fallas en el equipamiento, interrupción de energía eléctrica, inundación de instalaciones, y demás que afecten los activos de información de **ASPAEN**.

Se deben evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del periodo de recuperación, se deben identificar los

recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y especificar las prioridades de recuperación.

7.10.2. Acuerdos de nivel de servicio

El Oficial de Seguridad de la Información y el área legal de **ASPAEN** revisarán los contratos o acuerdos existentes con los proveedores de servicio, teniendo los siguientes lineamientos:

1. Cumplir con la Política de Seguridad de la Información.
2. El acuerdo de confidencialidad de la información que sea compartida transmitida o gestionada.
3. Descripción de los servicios contratados. Nivel de servicio esperado de acuerdo con la naturaleza del servicio contratado y con las debidas multas ante el incumplimiento de los niveles pactados.

7.10.3. Segregación de ambientes

Los ambientes de desarrollo, prueba y operaciones estarán separados siguiendo las siguientes definiciones:

1. Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos o directorios.
2. Separar las actividades de desarrollo y prueba, en entornos diferentes.
3. Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo.
4. Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas.
5. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
6. Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.
7. El personal de desarrollo no tendrá acceso al ambiente operativo.

7.10.4. Gestión de cambios

Se deben definir los procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en lo relativo a los aspectos de riesgos técnicos y/o de seguridad. Se deberá controlar que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de estos ni de la información que soportan.

Los procedimientos de cambio evaluarán el posible impacto operativo de los cambios previstos y verificará su correcta implementación. El Responsable del Sistema de Información mantendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios deberán contemplar los siguientes puntos:

1. Evaluación de los riesgos del posible impacto de los cambios.
2. Aprobación formal de los cambios propuestos.

3. Planificación del proceso de cambio – Ingeniería del detalle.
4. Prueba del nuevo escenario.
5. Comunicación de detalles de cambios a todas las personas pertinentes.
6. Identificación de las responsabilidades.
7. Actividades de retorno ante imprevistos.

7.11. REGISTRO Y AUDITORÍA

El responsable de efectuar la auditoría y registro de los hallazgos evidenciados será el Oficial de Seguridad de la Información de **ASPAEN.**

La auditoría será llevada a cabo semestralmente, debiéndose levantar un acta de los hallazgos que se evidencien, de tal manera que se administre un registro consecutivo del cumplimiento de esta obligación.

7.12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

7.12.1. Nivel de impacto de los incidentes de seguridad

Dentro del Manual para la Gestión de Incidentes de Seguridad de **ASPAEN**, el impacto del incidente de seguridad es clasificado de la siguiente manera:

1. **Crítico**: Interrupción total de servicios críticos o compromiso significativo de los Datos Sensibles.
2. **Alto**: Impacto parcial en servicios o Datos.
3. **Moderado**: Afectación menor, sin comprometer servicios críticos.
4. **Bajo**: Incidentes que no representan un riesgo inmediato.

7.12.2. Protocolo de respuesta en el manejo de incidentes de seguridad

El Manual para la Gestión de Incidentes de Seguridad de **ASPAEN** tiene el propósito de establecer un marco sistemático para identificar, analizar, gestionar y resolver los incidentes de seguridad de la información que permita la continuidad del negocio y la protección de los activos de la información de la organización.

El protocolo para la gestión de incidentes de seguridad dispuestos al interior de **ASPAEN**, se presentan en las siguientes fases:

PROTOCOLO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD EN ASPAEN	
Fases	Descripción
Identificación del incidente	Permite a **ASPAEN** estar en capacidad de responder ante los incidentes asociados al Tratamiento de Datos Personales por medio de las siguientes actividades: 1. El monitoreo continuo de los sistemas mediante herramientas de detección de intrusión y antivirus. 2. El reporte y registro de incidentes. Uso de un canal centralizado para reportar los incidentes (Ej. Correo electrónico, sistema de *tickets*, grupo de teams). 3. La definición de criterios para clasificar un evento como incidente de seguridad.

PROTOCOLO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD EN ASPAEN	
Fases	Descripción
	Para efectos de la identificación de un incidente de seguridad se sugiere tener en cuenta lo siguiente al interior de **ASPAEN**: 1. Definir un listado de fuentes generadoras de eventos que permita la identificación de un incidente de seguridad asociado al Tratamiento de Datos Personales. 2. Buscar estrategias con el fin de que el incidente no se propague y genere más daños. Las estrategias deben variar según el tipo de incidente asociado al Tratamiento de Datos Personales. 3. Definir el nivel de prioridad, la criticidad de impacto -el impacto actual y el impacto futuro-, con el fin de implementar una atención adecuada a los incidentes de seguridad asociados al Tratamiento de Datos Personales.
Clasificación y priorización del incidente	Se clasificación y priorizan los incidentes de acuerdo con su impacto. La clasificación utilizada al interior de **ASPAEN** es la siguiente: 1. Crítico: Interrupción total de servicios críticos o compromiso significativo de los Datos Sensibles. 2. Alto: Impacto parcial en servicios o Datos. 3. Moderado: Afectación menor, sin comprometer servicios críticos. 4. Bajo: Incidentes que no representan un riesgo inmediato.
Contención del incidente	La contención permite tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.[44] **ASPAEN** implementará medidas inmediatas para limitar el alcance del incidente como: 1. Aislar los dispositivos afectados. 2. Revocar credenciales comprometidas. 3. Bloquear accesos sospechosos.
Análisis e investigación	En esta fase se recolectan las evidencias relevantes del incidente, incluyendo los registros, capturas de tráfico de red y las configuraciones afectadas. Además, se implementan las medidas necesarias para determinar la causa raíz para determinar cómo ocurrió el incidente y qué vulnerabilidades fueron explotadas. Se sugiere que una vez sea analizado el incidente de seguridad, se incluya la erradicación de este. Es decir, la eliminación de los rastros que hubiera podido dejar

[44] Ministerio de Tecnologías de la Información y las Comunicaciones – Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Pag 20. https://gobiernodigital.mintic.gov.co/692/articles-150509_G21_Gestion_Incidentes.pdf

PROTOCOLO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD EN ASPAEN	
Fases	Descripción
	la causa del incidente y que puedan entrañar la ocurrencia de uno nuevo.[45]
Resolución y recuperación	Al dar respuesta al incidente de seguridad, se aplican soluciones para la eliminación de la causa del incidente tales como actualizaciones de software, configuraciones de seguridad y eliminación del malware. Parte del protocolo implica la restauración de los servicios afectados asegurando que los sistemas estén libres de amenazas.
Aprendizajes y mejora continua	Las actividades post incidentes se componen del reporte del Incidente asociado al Tratamiento de Datos Personales, de la verificación de las lecciones aprendidas, del diseño e implementación de medidas tecnológicas, disciplinarias y penales de ser necesarias, así como el registro en la base de conocimiento para alimentar los indicadores.[46] Dentro de **ASPAEN**, se actualizan las políticas y procedimientos de seguridad para prevenir incidentes similares en el futuro, por lo anterior, es necesario documentar los siguientes datos de cada incidente presentado: 1. La descripción del incidente. 2. La causa raíz y medidas correctivas. 3. El impacto en los sistemas y Datos. 4. El tiempo de resolución y lecciones aprendidas.

7.12.3. Puntos o personas de contacto

En el evento de considerar que la seguridad y/o privacidad de la información que administra **ASPAEN** se encuentra en riesgo de la ocurrencia de un incidente de seguridad, se deberá contactar de manera inmediata con el Oficial de Seguridad de la Información de la organización:

Oficial de Seguridad de la Información: Rafael Bedoya Rivas
Número de Contacto: 316-4721069
Correo electrónico: juridica@aspaen.edu.co

7.12.4. Reporte del incidente

ASPAEN como Responsable del Tratamiento de Datos Personales, está obligado a adoptar las medidas de seguridad necesarias y a su alcance para impedir el acceso no autorizado y la alteración de los Datos Personales. No obstante, en caso de que ocurra una violación a los códigos de seguridad, informará de dicha circunstancia a la Superintendencia de Industria y Comercio, de conformidad con los lineamientos establecidos al interior de la organización.
Para esto, el personal encargado de efectuar el reporte ante la Superintendencia de Industria y Comercio será el Oficial de Protección de Datos Personales.

[45] Ministerio de Tecnologías de la Información y las Comunicaciones – Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Pag 22. https://gobiernodigital.mintic.gov.co/692/articles-150509_G21_Gestion_Incidentes.pdf
[46] Ministerio de Tecnologías de la Información y las Comunicaciones – Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Pag 23. https://gobiernodigital.mintic.gov.co/692/articles-150509_G21_Gestion_Incidentes.pdf

7.12.5. Documentación y/o registro interno del incidente

En caso de que se presente un incidente de seguridad y/o privacidad de la información de **ASPAEN**, el Oficial de Seguridad de la Información deberá llevar un registro documental que incluya la siguiente información:

1. La descripción del incidente.
2. La causa raíz y medidas correctivas.
3. El impacto en los sistemas y Datos.
4. El tiempo de resolución y lecciones aprendidas.

Se sugiere incluir dentro de dicha descripción, también:

1. Registrar concretamente los Datos que se vieron comprometidos.
2. La categoría de los Titulares de la información.
3. La fecha y la hora del incidente de seguridad y/o del descubrimiento del incidente.
4. La descripción de las investigaciones adelantadas por el encargado.
5. Prueba del reporte efectuado ante la Superintendencia de Industria y Comercio, cuando fuese necesario.
6. Prueba de la comunicación realizada a los Titulares de la información, cuando sea necesario.

7.13. Capacitación y sensibilización en seguridad de la información

ASPAEN a través del Oficial de Seguridad de la Información y el Oficial de Protección de los Datos Personales, deberá poner en conocimiento de los demás miembros de la organización la presente Política de Seguridad y Privacidad de la Información, efectuando periódicamente sensibilizaciones sobre la importancia del Principio de Seguridad en el Tratamiento de la información que se efectúa por parte de la organización, y las implicaciones que traería el incumplimiento de este.

De las sensibilizaciones que se hagan al interior de la organización, se levantará un acta donde conste: fecha de realización, tema y participantes.

8. VIGENCIA

La presente Política rige a partir de la fecha de su aprobación.

Las modificaciones que se den a las Políticas acá descritas darán origen a una nueva versión del documento.

Dada en Bogotá D.C a los 23 días del mes de enero de 2025.

IVÁN DARÍO REYES FLÓREZ
C.C. 79.940.157 de Bogotá
Representante Legal Suplente
ASPAEN
NIT. 860.019.021-9