POLITICA DE PROTECCIÓN DE DATOS PERSONALES DE LA ASOCIACION COLOMBIANA DE UNIVERSIDADES ASCUN

1. Objetivos

Esta Política establece lineamientos generales para la protección y el tratamiento de datos personales, permitiendo un mayor nivel de confianza entre los encargados y los responsables del trámite con respecto al tratamiento de sus datos.

Informar a los titulares de las finalidades y transferencias a que están sujetos sus datos personales y las formas y formas de ejercer sus derechos.

2. Alcance

La Política de Protección y Tratamiento de Datos Personales se aplicará a todas las bases o archivos que contengan datos personales y que sean tratados por parte del responsable.

3. Identificación del responsable

Responsable	ASOCIACIÓN COLOMBIANA DE UNIVERSIDADES -ASCUN-
Ocupación	Promover la calidad académica, la autonomía universitaria, la difusión del conocimiento y la responsabilidad social, integrando a la comunidad académica mediante mecanismos de interrelación, asociatividad y diálogo con el Estado y la sociedad.
Dirección:	Calle 93 No. 16 - 43 Bogotá, Colombia
E-mail:	ascun@ascun.org.co ; protecciondedatos@ascun.org.co
Web Site	https://ascun.org.co/

4. Definiciones

- **Acceso autorizado:** Permiso dado a un usuario para usar ciertos recursos, generalmente después de ingresar un usuario y contraseña correctos.
- **Autenticación:** Proceso para verificar la identidad de un usuario.
- **Autorización:** Consentimiento previo, expreso e informado del Titular para tratar sus datos personales.
- **Aviso de privacidad:** Comunicación al Titular sobre las políticas de tratamiento de sus datos personales y las finalidades del tratamiento.
- **Base de Datos:** Conjunto organizado de datos personales.
- **Contraseña:** Seña secreta que permite el acceso autorizado a dispositivos o información.
- **Control de acceso:** Mecanismo que permite acceder a dispositivos o información mediante autenticación.
- **Copia de respaldo:** Copia de datos que permite su recuperación.
- **Dato personal:** Información que puede asociarse a una persona.
- **Dato público:** Información no privada ni sensible, como el estado civil o profesión.
- **Datos sensibles:** Información que afecta la intimidad del Titular o puede generar discriminación, como origen racial, salud o vida sexual.
- **Encargado del tratamiento:** Persona o entidad que trata datos personales por cuenta del responsable.
- **Identificación:** Proceso de reconocimiento de la identidad de los usuarios.
- **Incidencia:** Anomalía que afecta la seguridad de los datos.
- **Perfil de usuario:** Grupo de usuarios con acceso a ciertos recursos.
- **Recurso protegido:** Componentes del sistema de información, como bases de datos o programas.

- **Responsable de seguridad:** Persona designada para controlar y coordinar las medidas de seguridad.
- **Sistema de información:** Conjunto de bases de datos y equipos para tratar datos personales.
- **Responsable del tratamiento:** Persona o entidad que decide sobre el tratamiento de los datos.
- **Soporte:** Material donde se registra o guarda información.
- **Usuario:** Persona autorizada para acceder a datos o recursos.
- **Titular:** Persona cuyos datos personales son tratados.
- **Tratamiento:** Operaciones sobre datos personales, como recolección o uso.
- **Transferencia:** Envío de datos personales a un receptor dentro o fuera del país.
- **Transmisión:** Comunicación de datos personales para su tratamiento por un encargado.

5. Marco Normativo de la Política de Protección de Datos Personales

En cumplimiento de las disposiciones legales vigentes en Colombia sobre protección de datos personales, la presente política se basa en las siguientes normas fundamentales:

1. **Ley Estatutaria 1581 de 2012**; Por la cual se dictan disposiciones generales para la protección de datos personales"; la cual desarrolla el derecho constitucional de todas las personas a conocer, actualizar y rectificar las informaciones recopiladas sobre ellas en bases de datos o archivos. También regula derechos como el de la intimidad y el acceso a la información, en los términos de los artículos 15 y 20 de la Constitución Política.
2. **Ley 1273 de 2009**; Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado 'de la protección de la información y de los datos', mediante la cual se introduce modificaciones al Código Penal para proteger la información y los datos personales, considerando las tecnologías de la información como un bien jurídico integral que merece especial tutela frente a posibles delitos cibernéticos.
3. **Decreto 1377 de 2013**; Por medio del cual se reglamenta parcialmente la Ley 1581 de 2012", la cual señala las directrices para la implementación de la Ley 1581 de 2012, incluyendo aspectos relacionados con el consentimiento informado y las medidas para garantizar la protección de los datos personales tratados por las organizaciones.
4. **Decreto 1074 de 2015**: Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo", la cual contiene disposiciones específicas para promover la competitividad, integración y desarrollo de los sectores productivos, entre ellos, la regulación en materia de protección de datos personales como parte del fortalecimiento del sector empresarial.

5. Política de Protección de datos Personales

La Asociación Colombiana de Universidades (ASCUN), comprometida con los principios de calidad académica, autonomía universitaria, difusión del conocimiento y responsabilidad social que conforman su misión, declara el cumplimiento íntegro de la Ley 1581 de 2012 y demás disposiciones reglamentarias en materia de protección de datos personales.

ASCUN adopta medidas técnicas, organizativas y legales que garantizan el tratamiento responsable de la información personal recolectada en el marco de sus actividades. Estas medidas están diseñadas para respetar los derechos de los titulares, así como los principios de finalidad, seguridad y confidencialidad establecidos por la ley bajo un enfoque que privilegia la protección de la información personal.

6. Principios de la protección de datos personales

En el ámbito de la protección de datos personales, se establecerán los siguientes principios fundamentales:

- **Principio de legalidad**: El tratamiento de datos, conforme a la Ley de Habeas Data, es una actividad regulada que debe ajustarse a lo estipulado en dicha ley y en las normas complementarias que la desarrollen.
- **Principio de finalidad:** La actividad de tratamiento debe responder a una finalidad legítima, conforme a la Constitución y la ley, la cual deberá ser comunicada al Titular de los datos.
- **Principio de libertad:** El tratamiento de datos solo podrá llevarse a cabo con el consentimiento previo, expreso e informado del Titular. No se permitirá la obtención o divulgación de datos personales sin la autorización adecuada, a menos que exista un mandato legal o judicial que exima ese consentimiento.
- **Principio de veracidad o calidad:** La información que se somete a tratamiento debe ser veraz, completa, exacta, actualizada, verificable y comprensible. Se prohíbe el tratamiento de datos que sean parciales, incompletos, fragmentados o que generen confusiones.
- **Principio de transparencia:** Durante el tratamiento, se debe garantizar el derecho del Titular a acceder, en cualquier momento y sin restricciones, a información sobre la existencia de datos que le afecten, proporcionada por el responsable o el encargado del tratamiento.
- **Principio de acceso y circulación restringida**: El tratamiento de datos se encontrará sujeto a límites derivados de la naturaleza de la información personal, así como de las disposiciones legales y constitucionales correspondientes. Esto implica que solo las personas autorizadas por el Titular y/o aquellas designadas por la ley podrán llevar a cabo dicho tratamiento. Exceptuando la información pública, los datos personales no estarán disponibles en Internet u otros medios de comunicación masiva, a menos que el acceso esté controlado técnicamente, garantizando que solo los Titulares o terceros autorizados por la ley tengan esa información.
- **Principio de seguridad:** La información sujeta a tratamiento por parte del responsable o del encargado, según lo establecido en la Ley de Habeas Data, deberá ser administrada con las medidas técnicas, humanas y administrativas necesarias para asegurar la protección de los registros, evitando su alteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- **Principio de confidencialidad:** Todas las personas que participen en el tratamiento de datos personales no públicos están obligadas a mantener la reserva de la información, incluso después de haber finalizado su relación con las actividades vinculadas al tratamiento. La comunicación o suministro de datos personales solo podrá realizarse en el marco de las actividades autorizadas por la ley y de acuerdo con los términos de esta política.

7. Derechos de los titulares

Los titulares de datos personales disfrutarán de los siguientes derechos, así como de aquellos que la ley les concede:

a. Conocer, actualizar y rectificar sus datos personales ante el responsable del tratamiento o los encargados de este. Este derecho se puede ejercer, entre otros casos, respecto a datos que sean parciales, inexactos, incompletos, fraccionados, que generen confusión, o aquellos cuyo tratamiento esté expresamente prohibido o no autorizado.
b. Solicitar una prueba de la autorización concedida al responsable del tratamiento, a menos que se exima explícitamente este requisito para el tratamiento, tal como se establece en el artículo 10 de la ley.
c. Ser informados por el responsable del tratamiento o el encargado, previa solicitud, sobre el uso que se ha dado a sus datos personales.
d. Presentar quejas ante la Superintendencia de Industria y Comercio por infracciones a las disposiciones de la ley y las normativas que la modifiquen, complementen o adicionen.
e. Revocar la autorización y/o solicitar la eliminación de sus datos cuando no se respeten los principios, derechos y garantías constitucionales y legales en el tratamiento. Esta revocación y/o eliminación procederá si la Superintendencia de Industria y Comercio determina que el responsable o el encargado han incurrido en conductas contrarias a la ley y la Constitución.
f. Acceder de forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

8. Roles y responsabilidades

La protección de datos personales en ASCUN se sustenta en una asignación clara de roles y responsabilidades. Cada actor dentro de la organización y aquellos relacionados de manera externa tienen funciones específicas que contribuyen al cumplimiento del marco legal y la salvaguarda de la información personal.

a. Comité de Calidad

El Comité de Calidad será el órgano responsable de supervisar, analizar y optimizar las políticas y procedimientos relacionados con la protección de datos en ASCUN. Este comité estará conformado por un delegado del Director Ejecutivo, el Oficial de Protección de Datos (DPO) y los líderes de áreas estratégicas.
Su principal misión será garantizar el cumplimiento normativo en materia de protección de datos, identificar riesgos asociados y proponer estrategias de mejora continua. El comité sesionará de manera ordinaria cada dos meses y, de forma extraordinaria, cuando se presenten emergencias o cambios significativos en la regulación.

b. Alta dirección

Los directivos y la dirección ejecutiva desempeñan un papel crucial en la protección de datos al ser responsables de proporcionar los recursos técnicos, humanos y financieros necesarios para implementar políticas robustas. Además, tienen la responsabilidad de liderar la adopción de las políticas internas y velar por el cumplimiento de los objetivos establecidos por el Comité de Calidad.

c. Oficial de Protección de Datos (DPO)

El Oficial de Protección de Datos tiene la responsabilidad de liderar la estrategia de cumplimiento en ASCUN, monitorear el correcto funcionamiento de los procesos relacionados y actuar como enlace entre la organización y las autoridades regulatorias. Adicionalmente, supervisará las auditorías internas y capacitará al personal sobre las mejores prácticas en el manejo de información.

d. Trabajadores

Cada trabajador tiene el deber de cumplir con las políticas establecidas por ASCUN en materia de protección de datos. Entre sus responsabilidades están participar activamente en las capacitaciones obligatorias, reportar cualquier incidente de seguridad y utilizar la información conforme a los principios de integridad, transparencia y confidencialidad.

e. Aliados y Contratistas

Los aliados estratégicos y contratistas que manejan información personal en nombre de ASCUN deben implementar medidas de protección, tanto administrativas como técnicas, para garantizar la seguridad de los datos. Asimismo, deben firmar acuerdos de confidencialidad y reportar cualquier incidente que comprometa la integridad de la información.

f. Responsable del Tratamiento

ASCUN, como responsable del tratamiento de los datos, tiene el deber de diseñar y ejecutar las políticas relacionadas con la recolección, almacenamiento, uso, transferencia y supresión de datos personales. Además, debe responder oportunamente a consultas y reclamos de los titulares y documentar las evidencias necesarias para demostrar el cumplimiento ante la Superintendencia de Industria y Comercio.

Son deberes del responsable:

- Garantizar al Titular el pleno y efectivo ejercicio de su derecho de hábeas data en todo momento.
- Solicitar y conservar, conforme a lo estipulado por la ley, una copia de la autorización correspondiente otorgada por el Titular.
- Informar adecuadamente al Titular sobre el propósito de la recolección de datos y los derechos que le asisten en virtud de la autorización concedida.
- mantener la información bajo las condiciones de seguridad necesarias para prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Asegurarse de que la información que se proporciona al Encargado del tratamiento sea veraz, completa, precisa, actualizada, verificable y comprensible.
- Actualizar la información, comunicando de manera oportuna al Encargado del tratamiento cualquier novedad respecto a los datos previamente suministrados, así como adoptar las medidas necesarias para mantener dicha información al día.
- Rectificar cualquier información incorrecta y comunicar los cambios pertinentes al Encargado del tratamiento.
- Proporcionar al Encargado del tratamiento únicamente aquellos datos cuyo manejo esté debidamente autorizado conforme a la legislación aplicable.
- Exigir en todo momento al Encargado del tratamiento el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- Tramitar las consultas y reclamos de acuerdo con lo indicado en la Ley Estatutaria 1581 de 2012.
- Adoptar un manual interno de políticas y procedimientos que asegure el cumplimiento adecuado de la ley, especialmente en la atención de consultas y reclamos.
- Informar al Encargado del tratamiento cuando determinada información esté en disputa por parte del Titular, siempre que se haya presentado la reclamación y el proceso respectivo no haya concluido.
- Proporcionar al Titular información sobre el uso que se da a sus datos, cuando así lo solicite.
- Notificar a la autoridad de protección de datos en caso de que se presenten violaciones a los códigos de seguridad y exista un riesgo en la administración de la información de los Titulares.
- Cumplir con las instrucciones y requerimientos impartidos por la Superintendencia de Industria y Comercio.
-

g. Encargado del Tratamiento

El encargado del tratamiento, que puede ser un área interna o un tercero contratado, tiene la responsabilidad de aplicar medidas de seguridad para evitar accesos no autorizados, fugas de información o pérdida de datos personales. También debe informar al responsable del tratamiento sobre cualquier irregularidad que se presente.

9. Autorización del tratamiento de los datos personales

Sin perjuicio de las excepciones establecidas en la Ley Estatutaria 1581 de 2012, como norma general, el responsable deberá obtener la autorización previa e informada del Titular para el tratamiento de datos personales. Esta autorización podrá ser recolectada a través de cualquier medio que permita su consulta posterior.

No será necesario contar con el consentimiento del Titular en los siguientes casos:

- Cuando la información sea solicitada por una entidad pública o administrativa en el ejercicio de sus funciones legales, o mediante orden judicial.
- Para datos de naturaleza pública.
- En situaciones de urgencia médica o sanitaria.

- Para el tratamiento de información autorizado por la ley con fines históricos, estadísticos o científicos.
- En relación con los datos que conforman el Registro Civil de las Personas.

10. Tipo de información recolectada

ASCUN recopila información personal de rectores, funcionarios y otros representantes de instituciones de educación superior en Colombia, así como de los participantes en actividades deportivas, culturales y de formación. Los datos recolectados incluyen nombres, apellidos, cargos y roles desempeñados en las universidades, así como información de contacto, principalmente correos electrónicos institucionales. En algunos casos, también se obtienen números de teléfono y datos específicos relacionados con los programas y áreas de interés de las instituciones representadas.

El propósito de esta recolección de información es facilitar la organización y gestión de eventos académicos, deportivos y normativos, así como garantizar una comunicación eficiente con rectores y funcionarios del sector educativo. Por ejemplo, ASCUN utiliza estos datos para enviar invitaciones a congresos, reuniones y socializaciones de normativas, además de coordinar citaciones a comités específicos y distribuir boletines informativos. En el ámbito deportivo, bajo la gestión de Red de Bienestar, se realizan registros de participantes en torneos y actividades, asegurando una adecuada y organizada documentación.

Además de los fines mencionados, ASCUN se compromete a proteger la información recopilada mediante la implementación de medidas que cumplen con la normativa vigente. Los datos personales se utilizan de manera transparente y exclusivamente para actividades que están alineadas con los objetivos institucionales, reforzando así la confianza entre las instituciones asociadas y los titulares de los datos.

11. Datos de niños, niñas y adolescentes

ASCUN gestiona de manera directa e indirecta el tratamiento de datos personales de menores de edad en el marco de sus eventos y actividades culturales, académicas y deportivas. Este tratamiento incluye la recopilación y el uso de información de estudiantes y deportistas menores, de manera responsable y en cumplimiento de la normativa vigente sobre protección de datos personales en Colombia.

Los datos recopilados son esenciales para facilitar el registro y la participación de los estudiantes y deportistas en eventos tales como competencias deportivas, congresos culturales y actividades académicas promovidas por ASCUN. Además, esta información permite garantizar una organización adecuada de las actividades, así como el cumplimiento de los requerimientos logísticos y legales asociados a cada evento.

ASCUN utiliza estos datos para fomentar la integración y la representación de los estudiantes en escenarios nacionales e internacionales, promoviendo su desarrollo integral a través de oportunidades deportivas y culturales. Asimismo, el tratamiento incluye el manejo de datos necesarios para gestionar becas, programas de intercambio y movilidad estudiantil, especialmente en el contexto de actividades universitarias organizadas por ASCUN y Red de Bienestar.

Un aspecto relevante es la promoción de la participación de los menores en actividades recreativas y competitivas, tanto culturales como deportivas. Para ello, ASCUN también utiliza imágenes y videos capturados durante los eventos con fines institucionales y académicos, siempre garantizando el respeto por los derechos de los menores y contando con el consentimiento necesario de los padres o tutores legales.

La información tratada se emplea además para mantener una comunicación con los padres o tutores de los estudiantes menores, compartiendo detalles importantes sobre la logística de las actividades, resultados y cualquier aspecto relevante para su participación.

ASCUN también lleva a cabo el tratamiento de los datos personales de niños, niñas y adolescentes que son hijos de sus trabajadores, de manera directa e indirecta, con el fin de gestionar su afiliación al Sistema de

Seguridad Social Integral, ejecutar actividades de bienestar laboral, y facilitar su inclusión en programas o beneficios organizacionales relacionados con la relación laboral. Este tratamiento se realiza en cumplimiento de las normativas legales vigentes en materia de protección de datos personales y con el propósito de garantizar el acceso a servicios y beneficios que contribuyan al bienestar de los trabajadores y sus familias. Para ello, ASCUN garantiza que toda la información recopilada será tratada bajo estrictas medidas de seguridad y confidencialidad, previa autorización explícita de los padres o representantes legales, y se limitará exclusivamente a los fines previamente mencionados.

12. Finalidades del tratamiento de datos

Denominación base de datos	Finalidades
TRABAJADORES, ASPIRANTES Y EXTRABAJADORES	Registrar y gestionar información de identificación personal, contacto, datos académicos, historial laboral, profesional y financiero de empleados, extrabajadores y aspirantes a cargos vacantes; desarrollar procesos de registro, vinculación y actualización de información, incluyendo a familiares como pareja, padres e hijos; implementar acciones de bienestar laboral, como programas recreativos y beneficios sociales; difundir ofertas laborales internas y gestionar procesos de selección, citando a entrevistas, verificando referencias y trayectoria profesional; realizar inscripciones y seguimiento en eventos, congresos y seminarios organizados por la asociación; enviar comunicaciones institucionales mediante correos electrónicos y mensajes de texto; entregar dotaciones y equipos asignados a colaboradores; afiliar al Sistema de Seguridad Social Integral (SSSI) y cajas de compensación; ejecutar actividades estadísticas, auditorías internas y externas; generar certificaciones laborales, de ascenso, traslado o entrevistas de retiro;; verificar información en listas restrictivas internacionales, como las de ONU y OFAC, para procesos de debida diligencia bajo el Programa de Transparencia y Ética Empresarial (PTEE); proporcionar datos a empresas con convenios para gestionar reservas y logística; gestionar la desactivación de sistemas de información al finalizar la relación laboral; y garantizar el cumplimiento de normativas legales aplicables a la protección de datos.
DIRECTIVOS DE IES ASOCIADAS Y NO ASOCIADAS	Asegurar la correcta vinculación y el registro de las Instituciones de Educación Superior (IES) como miembros de ASCUN, manteniendo una base de datos actualizada que incluya información relevante sobre sus representantes, contactos y áreas clave; facilitar la planificación y convocatoria para congresos, talleres, reuniones, foros, seminarios y otros eventos académicos, culturales y deportivos promovidos por ASCUN, con el propósito de fortalecer la colaboración entre instituciones; Difundir normativas, políticas públicas y avances legislativos y académicos que afecten a las IES, fomentando así el fortalecimiento del sistema educativo; realizar análisis, estudios e informes sobre tendencias, necesidades y proyecciones de las IES asociadas, contribuyendo a la generación de conocimiento que guíe decisiones estratégicas en beneficio del sector educativo; enviar boletines informativos, reportes, invitaciones y anuncios relevantes a las IES, promoviendo el intercambio de buenas prácticas y la participación activa en las iniciativas de ASCUN; Apoyar los procesos administrativos necesarios para asegurar la prestación adecuada de servicios a las IES asociadas, atendiendo consultas, solicitudes y trámites institucionales; Atender los

Denominación base de datos	Finalidades
	requerimientos de las autoridades competentes y el cumplimiento de las disposiciones legales relativas a la protección de datos personales, garantizando la transparencia y responsabilidad en su manejo; Impulsar iniciativas conjuntas entre ASCUN y las IES asociadas que incluyan programas académicos, de investigación, culturales y deportivos, beneficiando tanto a los estudiantes como a la comunidad educativa. Establecer y mantener contacto con las vicerrectorías de las Instituciones de Educación Superior asociadas, con el propósito de invitarlas a participar en diversos espacios de diálogo, colaboración y actividades institucionales, compartir comunicados, boletines, invitaciones relacionadas con la gestión de las vicerrectorías.
RECTORES	Los datos personales de las secretarías de las rectorías de las Instituciones de Educación Superior (IES) asociadas serán tratados con el propósito de mantener una comunicación eficiente y garantizar la coordinación de actividades relacionadas con el sector de la educación superior. Esta información será utilizada para invitar a los rectores a eventos, reuniones y espacios de interés, así como para realizar el envío de documentos relevantes que contribuyan al desarrollo y fortalecimiento de la educación superior en Colombia. El tratamiento de estos datos personales se realizará bajo estrictas medidas de seguridad y conformidad con la normativa vigente, asegurando la transparencia, confidencialidad y uso adecuado de la información, con el fin de consolidar relaciones institucionales efectivas y promover iniciativas en beneficio de las IES asociadas.
REPRESENTANTES Y PARTICIPANTES DEL CONSORCIO COLOMBIA	Los datos personales de representantes legales y delegados serán utilizados para mantener actualizada la información necesaria para la gestión y organización de su participación en los diferentes espacios realizados en el marco del Consorcio Colombia. Este tratamiento de datos permite coordinar actividades, facilitar la comunicación institucional, y garantizar una adecuada planeación y ejecución de las iniciativas y eventos relacionados con el Consorcio Colombia.
VIDEOVIGILANCIA	Monitoreo y control del acceso, así como del movimiento de personas dentro de la asociación, además de gestionar el ingreso y salida de vehículos del parqueadero; Vigilancia de incidentes y disuasión de comportamientos irregulares; Supervisión y control de la calidad en la prestación de los servicios institucionales.
PROVEEDORES Y CONTRATISTAS	Realizar evaluaciones y seleccionar proveedores potenciales; Cumplir con aspectos tributarios y legales ante entidades públicas y regulatorias; Establecer relaciones comerciales para la adquisición de bienes o servicios; Gestionar el control y los pagos correspondientes por los bienes y servicios recibidos; Llevar a cabo evaluaciones cualitativas y cuantitativas sobre los niveles de servicio proporcionados por los proveedores; Comunicar políticas y procedimientos sobre la manera de hacer negocios con los proveedores; Controlar y registrar contablemente las obligaciones adquiridas con ellos; Realizar consultas, auditorías y revisiones vinculadas a la relación comercial con cada proveedor; Cumplir con obligaciones contractuales establecidas; Atender decisiones judiciales y disposiciones administrativas, fiscales y regulatorias; Transmitir información y datos personales durante procesos de auditoría con clientes o entidades administrativas; Enviar invitaciones a contratar y

Denominación base de datos	Finalidades
	gestionar las fases precontractuales, contractuales y poscontractuales; Extender invitaciones a eventos organizados por ASCUN o Cualesquiera otras finalidades expresamente estipuladas en las autorizaciones otorgadas por los propios proveedores.
REPRESENTANTES Y PARTICIPANTES REDES UNIVERSITARIAS • Red Colombiana de Internacionalización – RCI • Observatorio de Responsabilidad Social Universitaria - ORSU • Red Universitaria de Emprendimiento - REUNE • Red de Enseñanza del español como Lengua Extranjera - EnRedELE • Red de Extensión Universitaria - RNEU • Red de Lectura y Escritura en la Educación Superior – REDLEES • Red de Comunidades de Graduados • Red de Bienestar	Los datos personales de las oficinas de los que hacen parte de las redes de ASCUN, serán utilizados para enviar información relevante sobre las actividades realizadas por los nodos. Este tratamiento de datos tiene como finalidad fortalecer la comunicación y coordinación entre las instituciones, facilitando la difusión de eventos, proyectos, y demás iniciativas que contribuyan al desarrollo y colaboración en el ámbito nacional e internacional de la educación superior. Para el caso de la Red de Bienestar se registra la participación de los titulares en actividades organizadas por ASCUN. Este registro permite dar soporte documental a las constancias de participación, garantizando la precisión y veracidad de la información proporcionada. Además, asegura el cumplimiento de las disposiciones legales aplicables en materia de protección de datos personales. También se registran las inscripciones de estudiantes, exalumnos, personal de apoyo y funcionarios de las universidades para realizar un adecuado seguimiento a su participación en las etapas de clasificación de los Juegos Universitarios.
DELEGADOS DE REPRESENTACIONES	Las finalidades del tratamiento de datos personales incluyen establecer y mantener un canal de comunicación efectivo con los delegados de ASCUN, convocar a reuniones, eventos y actividades institucionales, respaldar la gestión administrativa y representativa de dichos delegados ante diversas instancias de carácter institucional, académico, gubernamental u otras pertinentes, y garantizar el adecuado cumplimiento de los objetivos institucionales en el marco normativo aplicable.
REPRESENTANTES DE ORGANIZACIONES ALIADAS	Establecer y mantener contacto con las organizaciones para invitarlos a diversos espacios y/o compartir conceptos relacionados a su competencia, participar en diversos espacios de diálogo y colaboración, así como remitirles documentos de interés relacionados con la educación superior.
REPRESENTANTES Y PARTICIPANTES OBSERVATORIO JURÍDICO Y DE SOSTENIBILIDAD	Establecer y mantener contacto con las secretarías generales y los actores jurídicos de las Instituciones de Educación Superior asociadas, con el propósito de invitarlos a participar en diversos espacios de diálogo y colaboración, así como realizar solicitudes relacionadas con conceptos de proyectos de ley y normativas aplicables al sector.
REPRESENTANTES DE LA COMISIÓN CENTRO DE DERECHOS REPROGRAFICOS -CDR	Establecer y mantener contacto con la comisión técnica elegida, con el objetivo de proporcionar información pertinente sobre reuniones y capacitaciones que se desarrollen en conjunto con el CDR, asegurando una comunicación fluida y eficaz para el cumplimiento de sus funciones.
INSCRITOS EN EVENTOS DE ASCUN	Realizar el seguimiento de las participaciones en los espacios organizados, con el objetivo de evaluar la asistencia, identificar oportunidades de mejora y garantizar el cumplimiento de los

Denominación base de datos	Finalidades
	objetivos establecidos para dichas actividades. Gestionar invitaciones y el envío de información relacionada con el proyecto, incluyendo reuniones, capacitaciones y actividades asociadas, con el propósito de fomentar la participación y asegurar una adecuada comunicación con los interesados.
PARTICIPANTES DEL PROGRAMA RETOS	Conservar un registro actualizado de las personas que han participado en los diferentes espacios de formación y sensibilización organizados por el Programa RETOS, con el fin de compartir información sobre nuevas experiencias de aprendizaje, así como recabar sus percepciones y/o sugerencias para el fortalecimiento continuo del Programa.
REPRESENTANTES DE MEDIOS DE COMUNICACIÓN	Relacionamiento con medios de comunicación del distrito y nacionales para la participación como voceros de las IES que representamos ante temas coyunturales de la educación superior. Así mismo mediante listas de difusión compartimos hechos noticiosos de ASCUN.
REPRESENTANTES DE PRENSA DE LAS IES	Compartir boletines de prensa y comunicados a los enlaces en las oficinas de comunicaciones de cada una de las IES que representamos.

13. Procedimiento para ejercer derechos relacionados con protección de datos personales

El Titular, sus causahabientes, su representante y/o apoderado, o quien se determine por estipulación a favor de otro; podrá hacer ejercicio de sus derechos contactándose con nosotros a través de comunicación escrita a **protecciondedatos@ascun.org.co**.

13.1. Consultas

Los interesados podrán acceder a la información personal y a todos los datos registrados que estén vinculados con su identidad. Una vez que la Asociación reciba la consulta, se atenderá en un plazo máximo de diez (10) días hábiles, contados a partir de la fecha de recepción. Si por alguna razón no se puede responder dentro de este término, se comunicará al interesado informándole sobre los motivos de la demora y se establecerá una nueva fecha para atender la consulta, la cual no podrá exceder los cinco (5) días hábiles adicionales.

13.2. Reclamos

En caso de que se considere necesaria la corrección, actualización o eliminación de información contenida en una base de datos, o si se detecta el incumplimiento de los deberes establecidos por la Ley de Habeas Data, se podrá presentar un reclamo ante el responsable, siguiendo las siguientes pautas:

El reclamo deberá realizarse mediante una comunicación escrita enviada al correo **protecciondedatos@ascun.org.co**., incluyendo la identificación del titular, una descripción de los hechos que motivan el reclamo, la dirección de contacto, y cualquier documento que se considere relevante.

Si el reclamo se presenta incompleto, se notificará al interesado dentro de los cinco (5) días siguientes a su recepción para que subsane las deficiencias. Si, transcurridos dos (2) meses desde la solicitud de información adicional, el solicitante no presenta los datos requeridos, se entenderá que ha desistido del reclamo.

Si el responsable recibe un reclamo para el cual no tiene competencia, lo remitirá al área correspondiente en un plazo máximo de dos (2) días hábiles e informará al titular. Una vez que se reciba el reclamo completo, la Asociación incluirá en la base de datos una nota que diga "reclamo en trámite" junto con el motivo del mismo, en un plazo no mayor a dos (2) días hábiles.

El responsable mantendrá esta nota en el registro objeto de discusión hasta que se resuelva el reclamo. El plazo máximo para dar respuesta al reclamo será de quince (15) días hábiles a partir del día siguiente de su recepción. Si no es posible atenderlo en este período, la Asociación informará al titular sobre los motivos de la demora y sobre la nueva fecha para resolver su reclamo, que en ningún caso podrá superar los ocho (8) días hábiles posteriores al término inicial.

13.3. Contenido mínimo de la solicitud

Las solicitudes que el titular presente con el fin de realizar una consulta o reclamo respecto al uso y manejo de sus datos personales deberán incluir ciertas especificaciones mínimas. Esto se hace con el propósito de garantizar una respuesta clara y coherente. Los requisitos son los siguientes:

- Dirigida a la ASOCIACION COLOMBIANA DE UNIVERSIDADES -ASCUN-
- Identificación del titular (nombre y número de documento).
- Descripción de los hechos que originan la consulta o el reclamo.
- Objeto de la petición.
- Indicación de la dirección de notificación del titular, tanto física como electrónica (e-mail).
- Documentación que respalde la solicitud, especialmente en el caso de reclamos.

Si la consulta o reclamo se presenta de manera presencial, el titular deberá redactar su solicitud por escrito, cumpliendo únicamente con los requisitos mencionados anteriormente, sin necesidad de formalidades adicionales.

13.4. Requisito de procedibilidad

El titular, sus causahabientes, su representante y/o apoderado, o cualquier persona designada por acuerdo de las partes, podrá presentar una queja ante la Superintendencia de Industria y Comercio solo tras haber agotado el procedimiento de consulta o reclamo directamente con la Asociación.

13.5. Petición de actualización y/o rectificación

El responsable procederá a rectificar y actualizar, a solicitud del titular, la información que sea inexacta o esté incompleta, siguiendo el procedimiento y los términos previamente señalados. Para ello, el titular deberá enviar su solicitud a través de los canales establecidos por la Asociación, especificando la actualización o rectificación requerida, y anexar la documentación que respalde dicha petición.

13.6. Revocación de la Autorización y/o Supresión de Datos Personales

El Titular tiene el derecho de revocar en cualquier momento el consentimiento o autorización otorgada para el tratamiento de sus datos personales, siempre que no existan impedimentos establecidos por disposiciones legales o contractuales. Asimismo, el Titular puede solicitar en todo momento la supresión o eliminación de sus datos personales cuando:

A. Considera que sus datos no están siendo tratados de acuerdo con los principios, deberes y obligaciones estipulados en la normativa vigente.
B. Han dejado de ser necesarios o pertinentes para la finalidad para la que fueron recolectados.
C. Se ha cumplido el plazo necesario para los fines por los cuales fueron obtenidos. Esta supresión puede implicar la eliminación total o parcial de la información personal, según lo solicitado por el Titular en los registros, archivos, bases de datos o tratamientos realizados por el responsable.

Es importante señalar que el derecho a la cancelación no es absoluto y, por lo tanto, el responsable podrá negar la revocación de la autorización o la eliminación de los datos personales en los siguientes casos:

a) Si el Titular tiene un deber legal o contractual que lo obliga a permanecer en la base de datos;
b) Si la eliminación de los datos obstaculiza acciones judiciales o administrativas relacionadas con obligaciones fiscales, investigaciones y persecución de delitos, o la actualización de sanciones administrativas.
c) Si los datos son necesarios para proteger los intereses legalmente reconocidos del Titular, para llevar a cabo acciones en función del interés público o para cumplir con obligaciones legalmente adquiridas por el Titular.

14. Cesión, transferencia y transmisión de datos personales

14.1. Transferencia de Datos a Terceros Países

De acuerdo con el Título VIII de la Ley Estatutaria de Protección de Datos (LEPD), está prohibida la transferencia de datos personales a países que no garanticen niveles adecuados de protección. Se considera que un país ofrece un nivel adecuado cuando cumple con los estándares establecidos por la Superintendencia de Industria y Comercio, conforme a la Circular 005 del 10 de agosto de 2017. Estos estándares no podrán ser inferiores a los que la ley exige a sus destinatarios.

14.2. Excepciones a la Prohibición de Transferencia

No se aplicará esta prohibición en los siguientes casos:

1. Cuando el Titular haya otorgado su consentimiento expreso e inequívoco para la transferencia de sus datos.
2. En el intercambio de información de carácter médico que sea necesario para el tratamiento del Titular, por razones de salud o higiene pública.
3. En transferencias bancarias o bursátiles, según la legislación pertinente.
4. En transferencias acordadas dentro de tratados internacionales en los que la República de Colombia sea parte, basadas en el principio de reciprocidad.
5. Para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para llevar a cabo medidas precontractuales, siempre que se cuente con la autorización del Titular.
6. En transferencias que sean legalmente requeridas para proteger el interés público o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

14.3. Declaración de Conformidad

En aquellos casos que no sean considerados excepciones, será responsabilidad de la Superintendencia de Industria y Comercio emitir la declaración de conformidad respecto a la transferencia internacional de datos personales. El Superintendente tiene la autoridad para solicitar información y llevar a cabo las diligencias necesarias para verificar el cumplimiento de los requisitos que hacen viable esta operación.

14.4. Transmisiones Internacionales de Datos Personales

Las transmisiones internacionales de datos personales, que se realicen entre un responsable y un encargado con el fin de que este último lleve a cabo el tratamiento de los datos en nombre del responsable, no requerirán ser notificadas al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales que se ajuste a los siguientes requisitos:

a) Finalidad del Tratamiento: Especificar claramente el propósito del tratamiento de los datos personales por parte del encargado.
b) Obligaciones del Encargado: Establecer las responsabilidades específicas del encargado en cuanto a la protección y confidencialidad de los datos.
c) Derechos del Titular: Asegurar que el tratamiento de datos por parte del encargado no vulnerará los derechos del Titular conforme a la LEPD.

d) Medidas de Seguridad: Incluir las medidas de seguridad que el encargado deberá implementar para salvaguardar los datos personales durante su tratamiento.
e) Términos y condiciones: Es fundamental establecer claramente los términos y condiciones que regirán la transmisión de datos personales. Esto incluye la duración del tratamiento de dichos datos y las cláusulas que regirán la terminación del contrato.

14.5. Obligaciones adicionales para la transferencia internacional de datos:

a) **Evaluación del nivel de protección:** Antes de llevar a cabo cualquier transferencia, el responsable del tratamiento debe realizar una evaluación del nivel de protección de datos del país receptor, asegurándose de que este cumpla con los estándares fijados por la Superintendencia de Industria y Comercio.
b) **Notificación a la Superintendencia:** El responsable del tratamiento está obligado a comunicar a la Superintendencia de Industria y Comercio sobre la transferencia internacional de datos, proporcionando información detallada sobre las medidas implementadas para salvaguardar la protección de los datos personales.
c) **Documentación y registro:** Es imprescindible mantener un registro exhaustivo y una documentación detallada de todas las transferencias internacionales de datos. Esto incluye los contratos de transmisión, las evaluaciones de protección realizadas y las notificaciones enviadas.

15. Uso de cookies y datos de navegación

15.1. Cookies

ASCUN utiliza cookies para identificar las páginas que están siendo visitadas, con el objetivo de analizar el tráfico del sitio y mejorar su calidad. La información recopilada se destinará únicamente a fines de análisis estadístico; una vez alcanzados los objetivos establecidos en este documento sobre el tratamiento de datos personales, la información será eliminada del sistema.

15.2. Enlaces a otros sitios web y correo electrónico

El sitio web de ASCUN puede contener enlaces a otras páginas externas. Sin embargo, una vez que el usuario utiliza estos enlaces para salir del sitio principal, es importante tener en cuenta que la organización no tiene control sobre estos sitios ajenos. Por lo tanto, no se hace responsable de la protección y privacidad de la información que los usuarios proporcionen al visitar estos portales externos, quedando sujetos a las políticas de privacidad y manejo de datos de dichos sitios web.

15.3. Aceptación de la política de tratamiento de datos personales

La aceptación expresa de esta Política de Tratamiento de Datos Personales se considera válida cuando el cliente o usuario titular de la información proporciona sus datos en el sitio web de la Asociación, manifestando de manera autónoma y libre, ya sea oralmente, por escrito o a través de conductas inequívocas (ya sea de forma física o digital).

Para los fines de esta Política de Tratamiento de Datos Personales, se entiende por “tratamiento” cualquier operación o conjunto de operaciones realizadas sobre datos e información personal, tales como su uso, almacenamiento, recolección, transmisión y/o transferencia, según corresponda.

Al aceptar esta Política de Tratamiento de Datos Personales, cada titular de la información otorga su autorización de forma expresa a la Asociación para que procese los datos proporcionados, con el fin de cumplir con las finalidades que se describen en las bases de datos contenidas en este documento.

Respecto a las modificaciones de la política de privacidad y tratamiento de datos, la Asociación se reserva el derecho de realizar cambios o actualizaciones en esta Política de Tratamiento de Datos Personales en

cualquier momento. Esto puede responder a la necesidad de adaptarse a nuevas normativas, a políticas internas o a ajustes en los requisitos para la prestación y oferta de sus servicios y productos.

Cualquier modificación se hará accesible al público a través de medios digitales y/o físicos proporcionados por la Asociación, donde se publicará la versión actualizada y vigente de la Política de Tratamiento de Datos Personales.

16. Gestión de los riesgos

La gestión de riesgos en la protección de datos personales es una herramienta esencial que garantiza la seguridad, confidencialidad y legalidad en el tratamiento de información sensible. En este capítulo, se detallan las directrices necesarias para identificar, analizar y mitigar los riesgos inherentes y residuales asociados con las operaciones de manejo de datos, cumpliendo con la normativa colombiana vigente, específicamente la Ley 1581 de 2012 y el Decreto 1377 de 2013.

16.1. Identificación de Riesgos

ASCUN lleva a cabo la identificación de los riesgos inherentes vinculados al tratamiento de datos personales a través de un análisis exhaustivo de los procesos internos, los sistemas tecnológicos utilizados y la interacción con terceros. Algunos de los riesgos más comunes incluyen:

- Acceso no autorizado a datos personales.
- Pérdida o eliminación accidental de información.
- Incumplimiento normativo por falta de controles adecuados.
- Manejo inadecuado de información por parte de terceros.

Estos riesgos serán evaluados para determinar su posible impacto en la privacidad y seguridad de los titulares de los datos.

16.2. Análisis de Riesgos

El análisis de riesgos considera los siguientes aspectos:

a. Riesgo Inherente: Este representa el nivel de riesgo presente antes de la implementación de cualquier control o medida de seguridad, incluyendo amenazas naturales del entorno operativo.

b. Riesgo Residual: Se refiere al nivel de riesgo que continúa existiendo tras la aplicación de controles y medidas de mitigación, reflejando así la eficacia de las acciones implementadas.

Se emplearán matrices para estimar tanto la probabilidad como el impacto de cada riesgo, facilitando así la toma de decisiones informadas en relación con las medidas de mitigación a adoptar.

16.3. Control y Mitigación de Riesgos

ASCUN pondrá en práctica a corto, mediano y largo plazo una serie de controles para mitigar los riesgos identificados, tales como:

a. Medidas Administrativas: Establecimiento de políticas internas claras sobre el manejo de datos personales y capacitación continua para los colaboradores.
b. Medidas Tecnológicas: Implementación de herramientas de cifrado, autenticación multifactor y control de accesos.

c. Medidas Contractuales: Inclusión de cláusulas que aborden la protección de datos en los contratos con terceros.
d. Diseño de protocolos de respuesta ante incidentes, garantizando que la organización esté preparada para actuar ante cualquier eventualidad.

16.4. Monitoreo y Seguimiento

El monitoreo continuo es fundamental para mantener una gestión de riesgos efectiva. ASCUN adoptará indicadores clave de desempeño (KPIs) para evaluar la eficacia de los controles implementados, tales como:

- Número de incidentes relacionados con datos personales.
- Tiempo de respuesta ante eventos de seguridad.
- Grado de cumplimiento en auditorías internas y externas.

Este seguimiento permitirá identificar áreas de mejora y asegurar la actualización constante de los mecanismos de protección.

16.5. Responsabilidad Demostrada

En consonancia con el principio de responsabilidad demostrada, ASCUN documentará todas las actividades vinculadas a la gestión de riesgos, abarcando desde la identificación hasta el seguimiento de los controles. Esta documentación servirá como evidencia de cumplimiento ante las autoridades competentes y auditorías externas.

17. Seguridad de la información en ASCUN

La protección de datos personales es un derecho fundamental que garantiza a los titulares el control sobre su información personal. Este derecho les permite decidir quién puede acceder a sus datos, cómo serán utilizados y para qué fines. Además, asegura que puedan ejercer acciones como la consulta, corrección, eliminación y oposición al uso de su información.

La seguridad de la información de naturaleza personal se basa en tres columnas fundamentales:

- La Confidencialidad (para la persona correcta),
- La Integridad (información correcta) y,
- Disponibilidad (en el momento correcto).

En cumplimiento de lo establecido en la Ley 1581 de 2012, las medidas de seguridad adoptadas para el tratamiento de datos personales deben atender a diversos factores, tales como el riesgo inherente a la naturaleza de los datos, su nivel de sensibilidad, el desarrollo tecnológico disponible, y las posibles consecuencias para los titulares ante una eventual vulneración. Además, dichas medidas consideran aspectos como el volumen de titulares implicados, las transferencias de información realizadas y las experiencias previas relacionadas con la seguridad de los sistemas de tratamiento.

17.1. Medidas de seguridad

17.1.1 Medidas de seguridad técnicas

Las bases de datos de ASCUN son accesibles únicamente para las personas designadas en el ANEXO No. 1, de este documento. Los responsables de seguridad, también señalados en dicho anexo, son los encargados de gestionar los permisos de acceso de los usuarios, garantizando la confidencialidad, integridad y almacenamiento seguro de las contraseñas, así como la periodicidad de su cambio.

1. **Uso de Redes Privadas Virtuales (VPN):** Se emplean servidores virtuales para proteger las comunicaciones internas y garantizar un acceso seguro a los datos. Adicionalmente, se mantienen respaldos de información mediante servicios tercerizados y copias locales realizadas de manera interdiaria.
2. **Seguridad Perimetral:** El sistema de seguridad perimetral firewall protege las redes internas contra accesos no autorizados. Este sistema incluye filtros avanzados que controlan el tráfico de red, previniendo amenazas externas.
3. **Gestión de Contraseñas:** Se fomenta el uso de contraseñas alfanuméricas robustas para garantizar una mayor protección contra accesos no autorizados. Una contraseña robusta debe cumplir con las siguientes características:
   - Longitud mínima: 8 caracteres.
   - Composición: Incluir letras mayúsculas y minúsculas, números, y al menos un carácter especial (por ejemplo: @, #, %, &, *).
   - Ejemplo: M1cr0@1!
   - Las contraseñas de equipos, redes Wifi-internas y otros sistemas críticos, deben ser modificadas al menos cada seis meses.

4. **Gestión de Usuarios y Contraseñas**: El área de sistemas deberá garantizar la desactivación inmediata de usuarios y contraseñas de cualquier sistema o recurso interno al momento de finalizar la relación laboral o contractual de una persona con ASCUN. Además, se deberá realizar un registro formal de estas desactivaciones, incluyendo fecha y hora de la acción, para asegurar trazabilidad y cumplimiento de las políticas de seguridad.
5. **Control de Equipos Personales**: Los equipos personales están sujetos a filtros VPN, se solicita a los usuarios mantener actualizados sus antivirus y aplicar medidas básicas de seguridad, como instalar actualizaciones del sistema.
6. **Respaldo de Información**: Se realizan respaldos locales interdiarios para garantizar la recuperación de la información en caso de incidentes. Estos respaldos se almacenan en ubicaciones protegidas dentro de las instalaciones.

17.1.2 Medidas de seguridad físicas

1. **Control de Acceso a Áreas Restrictivas:** Se garantiza que solo el personal autorizado tenga acceso a zonas donde se maneja información sensible. Este control se implementa mediante llaves, tarjetas de acceso o códigos de seguridad, y se registra cada ingreso y salida en un registro físico o digital.
2. **Protección de Documentos Físicos**: Los documentos que contienen información sensible se almacenan en archivadores bajo llave, ubicados en oficinas seguras. Además, se clasifican por nivel de sensibilidad para garantizar que solo el personal autorizado tenga acceso a ellos.
3. **Monitoreo con Cámaras de Seguridad**: Las áreas clave, como entradas y salas de archivo, se monitorean mediante cámaras de seguridad instaladas estratégicamente. Las grabaciones son revisadas periódicamente para identificar y prevenir posibles incidentes.
4. **Seguridad en el Transporte de Información Física**: La salida de documentos sensibles de las instalaciones se realiza únicamente con autorización previa por parte del oficial de protección de datos. Los documentos se transportan con medidas seguras para garantizar su integridad durante el traslado.
5. **Protección de Equipos Tecnológicos**: Los equipos críticos están ubicados en espacios cerrados y seguros, a los cuales solo tiene acceso el personal autorizado.
6. **Gestión de Emergencias**: Se cuenta con un plan de respuesta ante emergencias como incendios o desastres naturales, que incluye rutas de evacuación y medidas específicas para proteger documentos importantes. Además, se mantienen extintores disponibles en áreas estratégicas.
7. **Inspecciones Periódicas**: Las instalaciones se revisan frecuentemente para detectar y corregir riesgos como cerraduras dañadas o cámaras fuera de posición. Estas inspecciones se documentan para garantizar la solución inmediata de los problemas encontrados.

17.1.3 Medidas de seguridad administrativas

1. **Políticas de Seguridad de la Información:** Establecer políticas claras sobre el manejo, almacenamiento y uso de la información. Estas políticas deben ser difundidas entre todo el personal y revisadas periódicamente para garantizar su actualización y cumplimiento.
2. **Confidencialidad y Acuerdos de Privacidad:** Todo el personal que tenga acceso a información sensible debe firmar acuerdos de confidencialidad, comprometiéndose a proteger los datos y evitar su divulgación. Esto incluye empleados, contratistas y terceros que interactúen con la información.
3. **Clasificación y Manejo de la Información:** Implementar procedimientos para clasificar la información según su nivel de sensibilidad (pública, privada o confidencial). Esto permite establecer controles específicos dependiendo del tipo de dato y su criticidad.
4. **Capacitación y Concienciación:** Realizar sesiones de capacitación periódicas para el personal en temas de protección de datos, ciberseguridad y buenas prácticas de manejo de información. Además, fomentar una cultura organizacional centrada en la seguridad de la información.
5. **Gestión de Accesos y Roles:** Definir y asignar roles y responsabilidades claras respecto al acceso a la información. Esto incluye asegurar que cada usuario solo tenga acceso a los datos necesarios para cumplir con sus funciones laborales.
6. **Auditorías y Revisiones Periódicas:** Realizar auditorías internas para identificar riesgos, verificar el cumplimiento de políticas y detectar posibles brechas de seguridad. Estas auditorías permiten ajustar las medidas administrativas según las necesidades actuales de ASCUN.
7. **Control de Salida de Información:** Establecer procesos claros para la autorización y registro de la salida de información fuera de la organización, ya sea en formato físico o digital. Esto incluye la supervisión de correos electrónicos, dispositivos portátiles y otras herramientas de transferencia de información.
8. **Gestión de Incidentes:** Se cuenta con un protocolo de respuesta ante incidentes de seguridad de la información, asegurando que exista un procedimiento claro para reportar, investigar y resolver cualquier posible vulneración.

18 Modificación de las políticas

Nos reservamos el derecho de modificar nuestra Política de Tratamiento y Protección de Datos Personales en cualquier momento. No obstante, cualquier cambio será comunicado oportunamente a los titulares de los datos a través de los canales de contacto habituales, con un plazo de diez (10) días hábiles antes de que las modificaciones entren en vigor. En caso de que un titular no esté de acuerdo con la nueva Política, ya sea general o específica, y tenga razones válidas que justifiquen su decisión de no continuar con la autorización para el tratamiento de sus datos personales, podrá solicitar a la Asociación el retiro de su información mediante el correo **protecciondedatos@ascun.org.co**. Sin embargo, los titulares no podrán solicitar la eliminación de sus datos personales si la Asociación tiene un deber legal o contractual de seguir tratándolos.

19 Sanciones por Infracciones a la Política de Protección de Datos Personales

El incumplimiento de lo establecido en esta Política de Protección de Datos Personales, así como de la normativa aplicable, puede resultar en la rescisión inmediata de las relaciones contractuales o comerciales en las siguientes situaciones:

a. Relaciones Laborales: Si un empleado comete infracciones graves a la Política de Protección de Datos Personales, la Asociación estará facultada para dar por terminado el contrato laboral por justa causa, de acuerdo con el reglamento interno de trabajo y las disposiciones del Código Sustantivo del Trabajo.

b. Acuerdos Comerciales o Civiles: En el caso de que un contratista, proveedor u otra parte vinculada mediante acuerdos civiles o comerciales no cumpla con las directrices de esta política, la organización podrá finalizar el respectivo acuerdo, previa notificación, de acuerdo con los términos estipulados en el contrato y la legislación aplicable.

c. Obligaciones Adicionales: Además de la posible terminación de las relaciones contractuales o comerciales, quienes incurran en incumplimientos pueden enfrentar acciones legales, que incluyen demandas civiles o denuncias penales, para la reparación de los daños causados a los titulares de los datos personales.

ASCUN se reserva el derecho de adoptar medidas correctivas y legales al detectar incumplimientos, con el objetivo de proteger los derechos de los titulares y cumplir con las disposiciones legales sobre la protección de datos.

20 Vigencia

La presente Política rige a partir del veintiocho (28) de marzo de 2025.

OSCAR DOMÍNGUEZ GONZÁLEZ
Representante Legal y Director Ejecutivo
Asociación Colombiana de Universidad ASCUN