POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
ACO CARIBE, S.A.

1. IDENTIFICACIÓN

Calidad	Responsable del tratamiento[1]
Razón social	ACO CARIBE, S.A.
Identificación	RUC: 155713427-2-2021 D.V. 94
Dirección	P.H. Pacific Center, Punta Pacífica, Torre A, Oficina 2000, Teléfono: 6751-0044.
Correo electrónico	rui.rebelo@aco.com

2. OBJETIVO

La presente política se elabora por **ACO CARIBE, S.A.** con el propósito de adoptar las medidas necesarias y conducentes a otorgar seguridad a los datos personales evitando o disminuyendo el riesgo de adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento y de cumplir estrictamente los principios de lealtad, finalidad, proporcionalidad, veracidad y exactitud, transparencia, confidencialidad, licitud, portabilidad.

3. CONTENIDO GENERAL

En la política de seguridad de la información de **ACO CARIBE, S.A.** se consagran medidas administrativas, técnicas y humanas para ejecutar el sistema de gestión de seguridad de la información, buscando establecer un marco de confianza en el ejercicio de sus deberes entre **ACO CARIBE, S.A.** y sus proveedores, clientes, personal y terceros vinculados, todo enmarcado en el estricto cumplimiento de las leyes.

4. NORMAS BASE

Las normas en virtud de las cuales se expide la presente política es la Ley 81 de 2019, de 26 de marzo de 2019 creada por la Asamblea de Diputados de la República de Panamá y publicada en la Gaceta Oficial No. 28743-A y su reglamentación mediante Decreto Ejecutivo No. 285 de 28 de mayo de 2021 publicada en la Gaceta Oficial No. 29296-A emitido por el Ministerio de la Presidencia.

5. PRINCIPIOS SOBRE PROTECCIÓN DE DATOS

De conformidad con la Ley 81 de 2019 reglamentada por el Decreto Ejecutivo No. 285 de 28 de mayo de 2021 establece los siguientes principios que serán aplicables a todas las bases de datos:

a. **Principio de lealtad**: Los datos personales deberán recabarse sin engaño o falsedad y sin utilizar medios fraudulentos, desleales o ilícitos.
b. **Principio de finalidad**: Los responsables del tratamiento deberán recolectar datos con fines determinados y legítimos. Los datos no podrán utilizarse posteriormente de manera incompatible o diferente con dichos fines.

[1] Ley 81 de 2021. Artículo 4° Numeral 17. Definiciones. Para los efectos de la presente ley, se entiende por: (Responsable del Tratamiento: Persona natural o jurídica, de derecho público o privado, lucrativa o no, que le corresponde las decisiones relacionadas con el tratamiento de los datos y que determina los fines, medios y alcance, así como cuestiones relacionadas a estos).

El tratamiento ulterior de los datos personales con fines de investigación, estudios, encuestas o conocimientos de interés público, no se considerará incompatibles con los fines que motivaron la recogida. Los fines del tratamiento de los datos determinarán el plazo de conservación de estos, transcurrido el cual el responsable del tratamiento los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización. Para determinar el plazo de conservación de los datos se acudirá a las leyes aplicables en cada caso y a las responsabilidades de todo orden que deban ser atendidas por el responsable del tratamiento o custodio de la base de datos. En el caso de datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias se atenderá a lo dispuesto en el artículo 30 de la Ley 81 de 2019.

c. **Principio de proporcionalidad**: Para conocer qué datos son adecuados, pertinentes y mínimos necesarios para la finalidad perseguida con el tratamiento de los datos, los responsables del tratamiento y, en su caso, los custodios de la base de datos, tomarán en cuenta el estado de la tecnología, la naturaleza, ámbito, contexto y fines del tratamiento.
   Con este fin podrán realizar y documentar evaluaciones de impacto en protección de datos personales con el objeto de minimizar los datos objeto de tratamiento, conocer los riesgos que impliquen los tratamientos y adoptar las medidas y garantías necesarias para mitigarlos.
   La autoridad de control podrá definir aquellos supuestos en los que es recomendable realizar una evaluación de impacto y establecer las pautas o estándares a seguir en su desarrollo. Los responsables del tratamiento y los custodios de las bases de datos, adoptarán medidas organizativas que regulen el acceso a los datos personales en su entidad, conforme a este principio permitiendo el acceso a ellos únicamente a los empleados o funcionarios públicos que lo necesiten para el desarrollo de sus funciones y limitando el mismo a la cantidad de datos y al tiempo necesario para ello.
d. **Principio de veracidad y exactitud**: Los responsables del tratamiento adoptarán las medidas necesarias para mantener exactos y puestos al día los datos personales en su posesión, de tal manera que no se altere la realidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.
e. **Principio de transparencia**: Toda información o comunicación al titular de los datos personales relativa al tratamiento de éstos deberá ser en lenguaje sencillo y claro, y mantenerlo informado de todos los derechos que el amparan como titular del dato, así como la posibilidad de ejercer los derechos ARCO.
f. **Principio de confidencialidad**: Todas las personas que intervengan en el tratamiento de datos personales están obligadas a guardar secreto o reserva respecto de estos, incluso cuando hayan finalizado su relación con el titular o responsable del tratamiento de los datos, impidiendo el acceso o uso no autorizado.
g. **Principio de licitud**: Para que el tratamiento de un dato personal sea lícito, deberá ser recolectado y tratado con base en algunas de las condiciones de licitud que reconocer la Ley 81 de 2019 y conforme a lo que se describe en la Sección tercera de este Capítulo.
h. **Principio de portabilidad**: El titular de los datos tiene derecho a obtener de parte del responsable del tratamiento una copia de los datos personales de manera estructurada en un formato genérico y de uso común.

6. ÁMBITO DE APLICACIÓN

La política de seguridad de información aplica a la información personal sobre la que **ACO CARIBE, S.A.** realiza cualquier tratamiento, en especial la información que reposa en las bases de datos digitales y físicas de la empresa.

7. DESTINATARIOS

De acuerdo con lo anterior, esta política está dirigida a **ACO CARIBE, S.A.** en consonancia con la Política de tratamiento datos -actualizada diciembre 2021- en particular a los trabajadores y terceros vinculados que tengan como función o sus actividades estén relacionadas con el tratamiento de datos personales recolectados y/o almacenados por la empresa, será de obligatorio cumplimiento y hará parte integral de loscontratos de trabajos.

8. PROPÓSITOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

a. Establecer las responsabilidades grupales e individuales frente a la seguridad de la información de las áreas y funcionarios de **ACO CARIBE, S.A.**
b. Proteger la información generada, recolectada, almacenada y tratada por **ACO CARIBE, S.A.**
c. Minimizar impactos financieros, operativos o legales debido a un uso incorrecto de la información personal recolectada y almacenada en las bases de datos de **ACO CARIBE, S.A.**
d. Implementar controles para el acceso a bases de datos a fin de garantizar la debida custodia.
e. Detectar de forma temprana incidentes de seguridad y reportes oportunos ante la Superintendencia de Industria y Comercio
f. Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

9. RESPONSABLES AL INTERIOR DE ACO CARIBE, S.A.

Los siguientes funcionarios han sido designados para el cumplimiento de la presente política:

ACTIVIDAD	CARGO / FUNCIONARIO
Aprobación de la política	Gerente
Implementación de la política: a. Estructurar, diseñar y administrar las medidas para la protección de la información a través de la política. b. Establecer los controles necesarios al interior de la empresa que garanticen la protección de la información. c. Coordinas las actividades requeridas con el personal de la empresa. d. Registrar y actualizar la información en el Registro Nacional de Bases de Datos -RNBD de la Superintendencia de Industria y Comercio. e. Obtener las declaraciones de conformidad de la SIC cuando sea requerido. f. Revisar los contenidos de los contratos cuando implique transmisión o transferencia internacional de datos personales. g. Incluir la política en los contratos de trabajo y demás contratos con terceros relacionados. h. Acompañar y asistir a la empresa en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio	Gerente
Publicación de la política	Gerente
Aplicación de la política	Gerente
Capacitación y entrenamiento sobre la política: a. Entrenamiento inicial b. Entrenamiento periódico	Gerente

Seguimiento y supervisión de la política: a. Controlar y actualizar bases de datos de la empresa. b. Seguimiento en particular sobre la recolección, almacenamiento, uso, circulación y supresión o disposición final de la información personal, incluyendo los requisitos para obtener la autorización de los titulares. c. Acceso y corrección de datos personales. d. Conservación y eliminación de información personal y bases de datos. e. Uso responsable de la información, incluyendo controles de seguridad f. Inclusión de acuerdos y cláusulas de confidencialidad y manejo de la información. g. Respuesta, gestión y seguimiento a las peticiones, quejas y reclamos elevados por los titulares de la información. h. Mantener organizada los archivos, material e información relacionada con esta política y la política de tratamiento de la información. i. Gestión de incidentes de seguridad. j.	Gerente
Actualización y revisión de la política	Gerente

10. POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN

ACO CARIBE, S.A. cuenta con una política de tratamiento de la información desde septiembre de 2016, actualizada a diciembre de 2021, adjunta alpresente documento e inscrita en el Registro Nacional de Bases de Datos -RNBD administrado por la Superintendencia de Industria y Comercio.

11. REVISIÓN PERIODICA

ACO CARIBE, S.A. realizará revisiones periódicas de la presente política, por lo menos una vez al año a fin de actualizarla, evaluarla y verificar los controlespara la seguridad de la información mediante la retroalimentación de los funcionarios de laempresa, contratistas y terceros relacionados.

12. PUBLICACIÓN:

La presente política ha sido difundida entre los funcionarios de **ACO CARIBE, S.A.** en conjunto con la política de tratamiento de la información una vez la misma fue revisada y aprobada para su implementación.

El documento estará disponible para su consulta en el servidor interno y físicamente se entregará a cada uno de los funcionarios de la empresa, que hará parte integral de su contrato de trabajo y de prestación de servicios, según corresponda.

13. INFORMACIÓN PERSONAL RECOLECTADA Y ALMACENADA POR ACO CARIBE,S.A.

ACO CARIBE, S.A. realiza tratamiento de la información personal de la siguiente manera:

GRUPO	INFORMACIÓN RECOLECTADA
TRABAJADORES	Nombres, identificación, datos de contacto, beneficiarios, información de fondo de pensiones, eps, referencias profesionales, referencias comerciales, información sobre nivel de educación, experiencia laboral, certificación bancaria
PROVEEDORES	Nombres, identificación, datos de contacto, certificación bancaria
CLIENTES	Nombres, identificación, datos de contacto, certificación bancaria
SOCIOS Y MIEMBROS DE JUNTA DIRECTIVA	Nombres, identificación, datos de contacto, certificación bancaria
CONTRATISTAS (Revisor fiscal, contador, abogado)	Nombres, identificación, datos de contacto, certificación bancaria

14. FINALIDADES DEL TRATAMIENTO DE LA INFORMACIÓN

En consonancia con la política de tratamiento de la información, las finalidades para las cuales **ACO CARIBE, S.A.** recolecta, almacena y accede a la información personal son las siguientes:

TRABAJADORES:

a. Tratar la información personal para el adecuado manejo de todos los procesos relacionados con Talento Humano dentro de **ACO CARIBE,S.A.**, así como para el envío de información relacionada con dichos procesos,tales como: Promover los procedimientos de verificación y evaluación de los aspirantes en los procesos de selección, control y seguimiento del proceso de contratación, Procesos de verificación y consulta de la veracidad de la información, referencias personales y/o laborales, antecedentes disciplinarios y/ojudiciales o aquellos relacionados con listas restrictivas de riesgos, prevención delavado de activos, corrupción y financiación del terrorismo. Soporte y ejecución de los beneficios colectivos derivados de un contrato de trabajo, tales como, perosin estar limitados a: la inscripción del colaborador y sus beneficiarios para la emisión de desprendibles de nómina o boletos de pago, afiliación y pago de las cotizaciones al sistema integral de seguridad social, inscripción y/o actualizaciónde beneficiarios ante el sistema integral de seguridad social, pago de la nómina,cursos de capacitación y formación, atención de actividades de bienestar, gestionar el sistema de seguridad y salud en el trabajo en el ejercicio de las diferentes actividades laborales y/o cualquier otro tipo de información relacionada directa e indirectamente el cumplimiento de las obligaciones derivadas de contrato de trabajo, contrato civil o comercial y con la administración del TalentoHumano;

b. Permitir el acceso a la información y datos personales a los auditores o terceros contratados para llevar a cabo procesos de auditoría interna o externa propios de la actividad que desarrolla **ACO CARIBE, S.A.;**

c. Consultar y actualizar la información y los datos personales, en cualquier tiempo, con el fin de mantener la veracidad de la información;
d. Contratar con terceros el almacenamiento y/o procesamiento de la información y datos personales para la correcta ejecución de los procesos y procedimiento propios de Talento Humano, bajo los estándares de seguridad y confidencialidad a los cuales estamos obligados.

PROVEEDORES Y CLIENTES:

a. **ACO CARIBE, S.A.** puede recolectar información y datos personales de los proveedores para cumplir de manera efectiva las obligaciones derivadas de la compra de bienes o contratación de servicios;
b. Comunicaciones y notificaciones relacionadas con el contrato o negocio jurídico que vincule a las partes;
c. Llevar a cabo evaluaciones y selección de proveedores potenciales;
d. Cumplimiento de aspectos fiscales y legales con entidades de gobierno y regulatorias;
e. Establecer relaciones de negocio para adquirir bienes o servicios;
f. Control y pagos por los bienes y servicios recibidos;
g. Evaluaciones cualitativas y cuantitativas de los niveles de servicio recibidos de los proveedores;
h. Comunicación de Políticas y procedimientos sobre la forma de hacer negocios con los proveedores;
i. Proceso de control y registro contable de las obligaciones contraídas con los proveedores;
j. Consultas, auditorias y revisiones derivadas de la relación de negocio con el proveedor;
k. Cualquier otra actividad necesaria para el efectivo cumplimiento de la relación comercial entre el proveedor y **ACO CARIBE, S.A.;**
l. Verificación en listas de riesgos o listas restrictivas, listas públicas, antecedentes disciplinarios, fiscales y penales;
m. Análisis financiero.

15. MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

a. Las directrices sobre el tratamiento de la información que realice **ACO CARIBE, S.A.** serán emitidas de forma exclusiva por la gerencia.
b. **ACO CARIBE, S.A.** elaborará e implementará la política de seguridad de la información conforme los estándares señalados en la normativa vigente.
c. Con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información, **ACO CARIBE, S.A.** empleará y distribuirá a susfuncionarios equipos y/o dispositivos móviles con los controles criptográficos.
d. **ACO CARIBE, S.A.** elaborará e implementará una política deuso de dispositivos móviles corporativos, en la que se incluye el objetivo, los destinatarios, identificación de los dispositivos entregados, determinación de los usos de dichos dispositivos, consecuencias del incumplimiento, compromisos de losfuncionarios y prohibiciones.

e. **ACO CARIBE, S.A.** llevará a cabo un procedimiento de identificación, uso, administración y responsabilidad frente a la información personalsobre la que realiza cualquier tratamiento.
   Identificación de la información: identificación y/o actualización de la información mediante la revisión de contratos, órdenes de compra y/o servicio con los clientes, proveedores y contratistas con el objeto de determinar la información que se requiere para la ejecución del contrato respectivo.
   Clasificación de la información: clasificación de la información de acuerdo a la criticidad, sensibilidad y reserva de la misma, siguiendo las definiciones de la Ley 81 de 2019 y Decreto Ejecutivo No. 285 de 28 de mayo de 2021.
   Uso: conforme a las finalidades previstas en esta política y en la política de tratamiento de la información.
   Administración: según se indique en el cuadro de funcionarios responsables en la implementación y aplicación de la presente política.
f. **ACO CARIBE, S.A.** mantendrá copias de seguridad digitales de la información a fin de asegurar su integralidad y evitando accesos, modificaciones o borrados no autorizados.
g. **ACO CARIBE, S.A.** implementará controles de acceso a los equipos, dispositivos y archivos en donde repose la información personal sobre la que realiza cualquier tratamiento.
   De esta forma se incluyen: uso de usuarios y contraseñas en cada equipo; uso de perfiles, usuarios y contraseñas para el acceso a la nube; uso de llaves para el acceso al archivo físico; acceso restringido a redes, aplicaciones y/o sistemas de información de la empresa; administración de usuarios y contraseñas por parte únicamente del gerente de la compañía, quien podrá crear, modificar y eliminar los mismos y deberá notificar a cada funcionario que los usuarios (ID) y contraseñas son personales e intransferibles y no deben prestarse, modificarse, eliminarse ni compartirse.
h. Trazabilidad: **ACO CARIBE, S.A.** implementará mecanismos que permitan la trazabilidad de las acciones que los funcionarios realicen sobre las bases de datos en donde conste la información personal.
i. Eliminación de la información: **ACO CARIBE, S.A.** implementará mecanismos que permitan la eliminación de la información personal que reposa en bases de datos físicas y digitales, como la adquisición de máquinas trituradoras de papel y procedimientos digitales de borrado de información sin almacenamiento de copias.
j. **ACO CARIBE, S.A.** realizará auditorías internas periódicamente para asegurarse de la implementación y aplicación de la presente política.
k. **ACO CARIBE, S.A.** celebrará acuerdos de confidencialidad y prohibición de circulación de información con funcionarios, proveedores, clientes ycontratistas.
l. **ACO CARIBE, S.A.** implementará mecanismos que permitanla gestión de incidentes de seguridad de la información que permita identificar la información personal filtrada, modificada o eliminada, reportar oportunamente a las personas implicadas y a la Superintendencia de Industria y Comercio, así como las medidas para disminuir el riesgo creado sobre la información personal.
m. **ACO CARIBE, S.A.** realizará capacitaciones a sus funcionarios sobre el manejo de la información personal que la empresa administre en su calidad de Responsable del tratamiento y evaluará a los trabajadores que tengan un rol específico en las actividades descritas en la presente política.

n. **ACO CARIBE, S.A.** implementará mecanismos que permitan la respuesta oportuna a las peticiones, quejas y reclamos de los titulares con respecto a cualquier aspecto del tratamiento.

16. INCUMPLIMIENTO

El incumplimiento de la presente política de seguridad de la información se considerará falta grave a los deberes de los trabajadores y será justa causa para terminar el contrato de trabajo.

De igual forma, en los contratos de prestación de servicios o de cualquier otra naturaleza, el incumplimiento es causal de terminación unilateral con justa causa y sin lugar a ningún tipo de indemnización y/o reconocimiento por daños y perjuicios.

17. VIGENCIA

La presente política de seguridad de la información de **ACO CARIBE, S.A.** entrará en vigencia a partir de su publicación y promulgación, diciembre 2021.