POLÍTICA CORPORATIVA DE PROTECCIÓN DE DATOS PERSONALES

1. ¿Quienes somos?

País	Nombre	RUC	Dirección
Ecuador	Cervecería Nacional CN S.A.	0990023549001	Kilómetro 16 ½ vía Daule, calle Cobre y avenida Pascuales, Edificio Cervecería Nacional, Guayaquil – Ecuador
Ecuador	Dinadec S.A.	0992526742001	
Ecuador	Tada Ecuador S.A.S.	0993370025001	
Ecuador	Beverage Brand & Patents Company BBPC S.A.	0993220574001	

Y cualquier otra compañía relacionada, a quienes en lo sucesivo se las denominará "las compañías".

2. ¿A qué nos comprometemos por medio de esta política?

Nos encontramos comprometidos a cumplir con la legislación vigente en materia de protección de datos personales, la cual nos obliga a cumplir determinadas exigencias, fundamentalmente referidas a:

- La recopilación y el uso de datos personales (en adelante, la "Información").
- La calidad y la seguridad de la información.
- Los derechos de las personas con respecto a la Información sobre sí mismos.

En este contexto, nos encontramos comprometidos con la protección, el manejo y el tratamiento adecuado de la Información a la que tiene acceso en la operación regular de sus negocios, ya sean datos de trabajadores, prestadores de servicios, clientes, proveedores, usuarios de los sitios web de las compañías, entre otros.

La presente política corporativa de protección de datos personales (en adelante, la "Política") recoge las prácticas desarrolladas por las compañías para la recolección, almacenamiento y tratamiento de Información a fin de asegurar el respeto por los derechos de sus titulares, así como el cumplimiento del marco normativo vigente.

La Política podrá ser complementada con reglamentos corporativos o directrices adicionales que desarrollen lo establecido en el presente documento siempre que se encuentren alineadas con sus principios rectores.

3. ¿En qué ámbito aplican las disposiciones de esta política?

El presente documento es aplicable a todas las bases de datos personales o información destinada a estar contenida en bases de datos de las compañías, así como al tratamiento de dichas bases de datos por parte de las compañías o por parte de terceros encargados.

Todos los trabajadores de todas las empresas que conforman las compañías se encuentran obligados a conocer y cumplir todas y cada una de las disposiciones de la Política.

4. Definiciones

Datos personales: toda información sobre una persona natural que la identifica o la hace identificable a través de medios que puedan ser razonablemente utilizados.

Datos sensibles: datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; pasado judicial; condición migratoria; identidad cultural; afiliación sindical e información relacionada a la salud o a la vida sexual e identidad de género.

Bases de datos personales: conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

Tratamiento de datos personales: cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

Titular de datos personales: persona natural a quien corresponden los datos personales.

Titular de la base de datos: persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido de la base de datos personales, el tratamiento de estos y las medidas de seguridad.

Encargado del tratamiento: persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular de la base de datos personales o el responsable de tratamiento.

5. ¿Quiénes son los responsables del cumplimiento de esta política?

El área responsable de revisar periódicamente la Política y efectuar los ajustes respectivos dentro de las compañías será definida por medio de la Política de Seguridad de la Información, la cual también incluye una relación detallada de las responsabilidades asignadas a las distintas áreas de las compañías para el cumplimiento de la normativa de protección de datos personales.

Sin perjuicio de ello, todos los empleados de las empresas que conforman las compañías, así como todos los terceros con quienes las compañías se vinculen en el ejercicio regular de su negocio y tengan acceso o realicen tratamiento de datos personales se encuentran sujetos al cumplimiento de la Política.

6. Confidencialidad

La Información a la que los trabajadores de las compañías y/o terceros tengan acceso tiene carácter confidencial y no podrá ser divulgada, comunicada ni compartida con terceros sin contar con el consentimiento previo del titular de la Información, salvo las excepciones establecidas en la Ley.

Todas las personas que intervengan en el tratamiento de la información están obligadas a guardar el secreto profesional y a mantener la confidencialidad respecto de estos. Dicha obligación se mantendrá aún después de finalizada la relación que une a esas personas con las compañías.

7. Principios

Las compañías se preocupan por que toda persona tenga el derecho a controlar la Información que comparte con terceros, así como el derecho a que ésta se utilice de forma apropiada. Por este motivo, en sus actividades regulares de negocio, las compañías respetan los principios establecidos en la legislación:

- Principio de legalidad: El tratamiento de la Información realizado por las compañías se realizará conforme a lo establecido en la Ley, demás normativa y jurisprudencia aplicable. Se encuentra prohibida la recopilación de información por medios fraudulentos, desleales o ilícitos.

- Principio de consentimiento: Las compañías no podrán tratar Información si no cuentan con el consentimiento previo, expreso, inequívoco y libre de su titular, salvo las excepciones previstas en la Ley.

- Principio de finalidad: La Información debe ser recopilada por las compañías para una finalidad determinada, explícita, lícita, legítima y comunicada al titular. El tratamiento de

dichos datos no se extenderá a una finalidad distinta a la establecida de manera inequívoca como tal al momento de su recopilación o incompatible con aquella que motivó su obtención.

- Principio de proporcionalidad: Todo tratamiento de la Información realizado por las compañías deberá ser adecuado, necesario, oportuno, relevante y no excesivo a la finalidad para la que la Información hubiese sido recopilada o a la naturaleza misma, de las categorías especiales de datos.

- Principio de calidad: La Información que vaya a ser tratada por las compañías debe ser veraz, exacta, íntegra, precisa, completa, comprobable, clara, y, en la medida de lo posible, actualizada, necesaria, pertinente y adecuada respecto de la finalidad para la que fue recopilada. Dicha Información deberá conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

- Principio de seguridad: Las compañías y los terceros que actúen como encargados del tratamiento de bases de datos personales de las compañías deberán adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de la Información y proteger los datos personales frente a cualquier riesgo, amenaza o vulnerabilidad. Éstas deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de la Información que se trate.

- Principio de nivel de protección adecuado: En el caso de que las compañías realicen transferencias internacionales de la Información deberá garantizar un nivel suficiente de protección para la Información que se vaya a tratar o por lo menos equiparable a lo establecido en la Ley.

- Principio de Lealtad: El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados.
  En ningún caso los datos personales podrán ser tratados a través de medios o para fines ilícitos o desleales.

- Principio de Transparencia: El tratamiento de datos personales deberá ser transparente, por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro. Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y se rigen en función

de las disposiciones contenidas en la presente Ley, su reglamento y demás normativa atinente a la materia.

- Principio de pertinencia y minimización de datos personales: Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento.

- Confidencialidad: El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley. Para tal efecto, el responsable del tratamiento deberá adecuar las medidas técnicas organizativas para cumplir con este principio.

- Principio de conservación: Los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento. Para garantizar que los datos personales no se conserven más tiempo del necesario, el responsable del tratamiento establecerá plazos para su supresión o revisión periódica. La conservación ampliada de tratamiento de datos personales únicamente se realizará con fines de archivo en interés público, fines de investigación científica, histórica o estadística, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales, oportunas y necesarias, para salvaguardar los derechos previstos en esta norma.

- Principio de responsabilidad proactiva y demostrada: El responsable del tratamiento de datos personales deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la presente Ley, para lo cual, además de lo establecido en la normativa aplicable, podrá valerse de estándares, mejores prácticas, esquemas de auto y corregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento. El responsable del tratamiento de datos personales está obligado a rendir cuentas sobre el tratamiento al titular y a la Autoridad de Protección de Datos Personales. El responsable del tratamiento de datos personales deberá evaluar y revisar los mecanismos que adopte para cumplir con el principio de responsabilidad de forma continua y permanente, con el objeto de mejorar su nivel de eficacia en cuanto a la aplicación de la presente Ley.

- Principio de aplicación favorable al titular: En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractuales, aplicables a la protección de datos

personales, los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de dichos datos.

8. Bases de datos de las compañías

Considerando las exigencias planteadas por la legislación en materia de protección de datos personales, las compañías cuentan con las siguientes bases de datos a ser registradas ante la Autoridad de Protección de Datos Personales:

Nombre	**Plazo de conservación**
Postulantes	Mientras resulten necesarios para cumplir con sus finalidades.
Trabajadores	Mientras resulten necesarios para cumplir con sus finalidades.
Clientes	Mientras resulten necesarios para cumplir con sus finalidades.
Consumidores finales	Mientras resulten necesarios para cumplir con sus finalidades.
Proveedores	Mientras resulten necesarios para cumplir con sus finalidades.
Bitácoras de acceso	Mientras resulten necesarios para cumplir con sus finalidades.
Videovigilancia	90 días

9. ¿Para qué tratamos datos personales en las compañías?

La información recopilada de los clientes y de consumidores finales se trata a efectos de ejecutar nuestra prestación de servicios. Adicionalmente, utilizamos esta información a fin de prestar servicios de mantenimiento y modificación técnica, facturación, entre otros.

La información recopilada sobre los postulantes a puestos de trabajo se utilizará para gestionar su candidatura a los puestos de trabajo ofrecidos por las compañías.

La información recopilada sobre los trabajadores se utilizará para gestionar la relación laboral que sostienen con las compañías incluyendo, pero sin limitarse a: las evaluaciones de desempeño, aptitudes, capacitación y desarrollo del trabajador; pruebas psicológicas, por competencias, la gestión de rendimiento, acciones correctivas e investigaciones.

La información recopilada sobre proveedores se utilizará para gestionar su relación comercial de prestación de servicios o comercialización de bienes a favor de las compañías.

La información recopilada por medio de nuestros sistemas de videovigilancia será utilizada a fin de preservar la seguridad de los establecimientos, bienes muebles e infraestructura.

La información recopilada por medio de nuestras bitácoras de acceso será utilizada a fin de preservar la seguridad de los establecimientos, bienes muebles e infraestructura mediante un control formal de accesos físicos en las instalaciones de las compañías de proveedores, clientes, trabajadores y demás visitantes.

En caso el titular de los datos personales haya dado su consentimiento para recibir contactos de naturaleza comercial, se le enviará encuestas de satisfacción, información de nuestros servicios, invitaciones a eventos, entre otros. Estos contactos se realizan principalmente a través de correo electrónico y eventualmente por mensajes de texto (SMS) y/o call center.

10. Derechos de los titulares de la Información

Las compañías contarán con un procedimiento sencillo y gratuito de atención de los derechos de los titulares de la Información contemplados en la Ley, entre ellos el derecho de acceso, actualización, rectificación, eliminación, oposición, portabilidad, entre otros.

Por lo tanto, las compañías realizarán las acciones necesarias para atender, de manera oportuna y dentro de los plazos, todas las solicitudes y requerimientos relacionados con dichos derechos.

En los procesos de atención de derechos de titulares de la Información serán de aplicación las siguientes directrices:

- La supresión o eliminación de la Información no procederá cuando ello afecte derechos o intereses legítimos de las compañías o cuando exista una obligación legal de conservación de la Información.

- Las compañías podrán rechazar determinados requerimientos cuando la divulgación de la información o la naturaleza del requerimiento pueda comprometer u obstaculizar actuaciones judiciales o administrativas en curso, entre otras situaciones.

Los titulares de los derechos podrán iniciar sus solicitudes por medio de una comunicación a las siguientes direcciones de correo electrónico: protecciondatosecuador@ab-inbev.com y/o gabriela.paredes@ab-inbev.com

Adicionalmente, podrán ejercer sus derechos de forma presencial, mediante el envío de una solicitud física, en la dirección consignada en el numeral 1) de esta política.

11. Transferencias de la Información

Las compañías podrán transferir datos personales a las compañías que formen parte del grupo Ab-InBev a nivel internacional, con la finalidad para la que la información fue recopilada y bajo previo consentimiento del titular, dicho consentimiento no será requerido en los supuestos permitidos por la normativa en materia de protección de datos personales.

La información objeto de tratamiento por parte de las compañías sólo será cedida o transferida a terceros para el cumplimiento de los fines relacionados con el interés legítimo del cedente y del cesionario, siempre que cuenten con el consentimiento previo, expreso, libre, inequívoco e informado del titular de la Información. Dicho consentimiento no será requerido en los supuestos permitidos por la normativa en materia de protección de datos personales.

Además de lo previamente establecido, las compañías no transferirán o comunicarán la Información a terceros, salvo en los siguientes casos:

a) Cuando sea necesario para la finalidad para la que la información fue recopilada.
b) Cuando se le informe al titular de la Información antes de la divulgación o al momento de la recopilación de la Información y se obtenga su consentimiento previo y expreso.
c) Cuando el consentimiento no sea exigido.
d) Cuando la Información sea requerida por entidades públicas en el ámbito de sus competencias y en el ejercicio de sus funciones y atribuciones.
e) Cuando la Información sea solicitada en virtud de órdenes judiciales o disposiciones legales.
f) Cuando se trate de acceso a la Información por parte de auditores, abogados y demás profesionales en ejercicio de sus funciones, obligados a guardar el secreto profesional.
g) Cuando los datos han sido recogidos de fuentes accesibles al público;
h) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica entre el responsable de tratamiento y el titular, cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con base de datos.
i) Cuando la comunicación se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando dichos datos se encuentren debidamente disociados o a lo menos anonimizados.
j) Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que implique intereses vitales de su titular y este se encontrare impedido de otorgar su consentimiento.
k) Cuando la comunicación de datos de carácter personal sea necesaria para realizar estudios epidemiológicos de interés público, dando cumplimiento a los estándares internacionales en la materia de derechos humanos.

12. Flujo transfronterizo o transferencia internacional de la Información

El flujo transfronterizo de la Información será posible cuando el receptor o importador de la Información asuma, en cuanto a la protección de la Información, las mismas obligaciones que corresponden al emisor o exportador, o cuando tenga legalmente autorización para ello.

13. Recopilación de datos sensibles

Las compañías únicamente recopilarán y tratarán Información y/o datos sensibles cuando sea estrictamente necesario, respetando los principios de finalidad y proporcionalidad y, únicamente bajo los supuestos que habilitan el tratamiento de datos sensibles de conformidad con la Ley.

14. Medidas de seguridad

Las compañías implementarán las medidas de seguridad técnicas y organizativas necesarias para garantizar la protección de la Información y evitar su alteración, pérdida, tratamiento y/o acceso no autorizado conforme a su Política de Seguridad de la Información.

En este sentido, las compañías cumplirán con la legislación vigente en materia de medidas de seguridad de protección de datos personales, específicamente en lo concerniente a los siguientes puntos:

- Control y registro de accesos y privilegios, así como su verificación periódica.
- Registro de eventos, interacciones lógicas,
- Identificación y autenticación de usuarios por medio de la gestión y uso de contraseñas.
- Copias y backup de la información de forma controlada y autorizada.
- Seguridad en los ambientes de procesamiento de datos personales.

En general las compañías y todos sus colaboradores que trabajen con datos personales cumplirán con las medidas de seguridad correspondientes a la naturaleza de la Información objeto de tratamiento de conformidad con lo establecido en la legislación.

15. Tratamiento por terceros – Encargados del tratamiento

Toda vez que las compañías encarguen el tratamiento de una base de datos a un tercero, o permita el acceso de terceros a sus bases de datos para la prestación de algún servicio específico, se deberán tener en cuenta las siguientes especificaciones:

- Todo tratamiento de la Información realizado por un tercero distinto a las compañías deberá estar regulado en un contrato, estableciéndose expresamente que el tratamiento de la

Información se realizará siguiendo las instrucciones de las compañías y, que únicamente se tratará la Información para los fines autorizados o establecidos en el contrato, por lo que el encargado no los utilizará con una finalidad distinta, ni los comunicará indebidamente a otras personas.

- El contrato deberá estipular las medidas de seguridad que el encargado del tratamiento está obligado a implementar, tales como la devolución o destrucción de la información una vez finalizado el encargo.

- El contrato deberá establecer que en caso de incumplimiento el infractor responderá ante el titular y ante las autoridades por todo tratamiento o uso no autorizado de la Información.

- Si el encargado del tratamiento necesita subcontratar con terceros para brindar parte de los servicios que se obligó a ofrecer, deberá contar con la autorización previa de las compañías y ésta sólo procederá siempre que el subcontratista asuma las mismas obligaciones que el encargado del tratamiento.

- El contrato deberá establecer además obligaciones de confidencialidad respecto a la información a la que accede el encargado del tratamiento, manteniéndose dichas obligaciones en vigor aún después de finalizado el plazo de vigencia del contrato.

16. Eliminación de la Información

Las compañías procederán a eliminar la Información de sus registros una vez que haya finalizado el tratamiento de la Información, se haya cumplido con el principio de finalidad, y no exista mandato legal o razón que justifique la conservación de la Información.

Alternativamente, se podrá aplicar procesos de disociación, anonimización o equivalentes cuando por alguna razón comercial, de estadística o de análisis de mercado se justifique la conveniencia de conservar la información.

Las compañías definirán oportunamente los procedimientos respectivos que resulten necesarios para la eliminación de la Información.

17. Auditoría Interna

Las compañías incorporarán el control de cumplimiento de la Política en los procesos regulares de auditoría interna.

18. Régimen de sanciones

La infracción cometida por un empleado a las previsiones establecidas en la Política se considerará una falta grave y susceptible de sanción. Las compañías tomarán las medidas disciplinarias que consideren pertinentes en los casos de incumplimiento de las obligaciones aquí estipuladas por parte de los empleados.

19. Difusión y cumplimiento de la Política

Las compañías procurarán: i) que se cumpla con lo dispuesto en la presente Política; ii) hacer conocer, observar y respetar la presente Política por cada empleado; iii) publicar la presente Política en lugares de fácil acceso; y iv) firmar convenios de confidencialidad con los empleados, usuarios, contratistas y terceros que accedan a la Información contenida en las bases de datos.

Fecha de última actualización: **28 de marzo de 2023.**