# POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION Y PROTECCION DE DATOS

Para CSCH SpA la Seguridad de la Información y Protección de Datos es un proceso continuo destinado a proteger los activos de información contra las amenazas internas y externas que pongan en peligro la integridad, disponibilidad, trazabilidad y/o confidencialidad de estos, donde se incluye también el Tratamiento de los Datos Personales que CSCH solicita a sus asociados y relacionados directos y/o aquellos que se recolectan de forma automática a través del sitio web www.cschcs.com y redes sociales asociadas, en cumplimiento con la legislación vigente en Chile y de los países donde CSCH realiza operaciones, y con los reglamentos y contratos acogidos por CSCH, su estrategia comercial y de negocios.

Toda información de CSCH, independiente del formato que tenga o de la forma en que se recolecte, debe ser protegida adecuadamente adoptando las medidas necesarias de Seguridad de la Información soportadas en los principios de integridad, disponibilidad, trazabilidad y confidencialidad de los datos, a través de la implementación de un conjunto de controles de prevención, detección y corrección que CSCH estructura en: (i) **Políticas**, directrices u orientaciones generales expresadas formalmente por la alta Gerencia; dirigidas al nivel estratégico, definen las reglas de alto nivel que representan los principios básicos, y servirán como base para que las normas y los procedimientos sean creados y detallados, asegurando que estos sean de carácter perpetuo, aunque se den cambios en la dirección y gestión de la compañía. (ii) **Normas**, disposiciones de carácter general que se desprenden de las Políticas de Seguridad de la Información, estableciendo obligaciones, restricciones, prohibiciones u otras conductas esperadas; dirigidas al nivel táctico, especifican las opciones tecnológicas y los controles que deben aplicarse para alcanzar la estrategia definida en las directrices de las políticas. (iii) **Procedimientos**, sucesiones cronológicas de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles definidos en las Políticas de Seguridad de la Información; están dirigidos al nivel operacional, describen las acciones para realizar las tareas citadas en las normas y las políticas.

En CSCH se entienden los principios de: (i) **Integridad**, como la garantía de que los datos se mantienen correctos y completos durante su almacenamiento, procesamiento y transmisión. Garantizar la integridad es adoptar las precauciones necesarias para que la información no sea modificada o eliminada sin autorización, por ello es necesario mantener la legitimidad y coherencia, de acuerdo con la realidad; cualquier falla en este punto, sea por una alteración o falsificación, quebrará la integridad. La violación en la integridad de la información puede causar impactos negativos a la compañía. (ii) **Disponibilidad**, como la propiedad de la información según la cual es accesible y utilizable oportunamente por los usuarios, sistemas o procesos autorizados, en el formato requerido para su procesamiento durante un periodo de tiempo determinado. Es muy importante para la compañía debido a que su negocio puede depender de la disponibilidad de los datos y sistemas para atender sus Socios Comerciales y Clientes. (iii) **Trazabilidad**, como los métodos para guardar registros (fechas, modificaciones y cambios en los datos, entre otros) de las acciones realizadas por los usuarios (trazas) para su posterior análisis. El objetivo es disponer de la información necesaria para poder auditar la seguridad de los sistemas. (iv) **Confidencialidad**, como la garantía de que sólo los usuarios previamente autorizados tienen acceso a determinada información, fuente o sistema de información. Eso significa que siempre que una información confidencial es accedida por un individuo no autorizado, intencionalmente o no, ocurre una "violación de la confidencialidad"; el quiebre de esa confidencialidad, dependiendo del contenido de la información, puede ocasionar daños inestimables a la compañía, sus Clientes, Socios Comerciales, Accionistas/Dueños, Socios y/o Colaboradores, e incluso a todo el mercado.

Las Políticas, Normas y Procedimientos de Seguridad de la Información y Protección de Datos de CSCH, no solo tienen en consideración a los avances tecnológicos, sino también a la evidente cultura de implementación de prácticas de seguridad. Por ello, integra requisitos de la norma ISO 27002:2022 "Seguridad de la información, ciberseguridad y protección de la

privacidad - Controles de seguridad de la información", abarcando en su implementación los cuatro ámbitos de control: (i) Controles Organizacionales, (ii) Controles de Personas, (iii) Controles Físicos y, (iv) Controles Tecnológicos; todo esto aunado a un marco conductual, ético y de seguridad descrito en nuestro Código de Ética y Conducta (leer en https://www.cschcs.com/codigo_etica_y_conducta.pdf), Política de Calidad y Seguridad en Cadenas de Suministro (leer en https:/www.cschcs.con/politica_de_calidad.pdf) y en esta Política General de Seguridad de la Información y Protección de Datos, sobre la cual CSCH establece un compromiso de mejora continua y, sobre sus fundamentos, exige a cada miembro de CSCH su deber de conocer, cumplir y hacer cumplir cabalmente las disposiciones que aquí se declaran.

CSCH también dará a conocer y exigirá las políticas de Seguridad de la Información y Protección de Datos a terceros con quienes se relacione, tales como Clientes y Socios Comerciales, que realicen trabajos para CSCH, incorporándose las cláusulas pertinentes en los contratos respectivos.

## SEGURIDAD DE LA INFORMACIÓN

Toda la información de CSCH sigue una clasificación definida según su tipo: (i) **Confidencial**, información crítica para el negocio de la compañía o de sus Clientes. La revelación no autorizada de dicha información puede causar impactos de tipo financieros, de imagen, operacional o, también, sanciones administrativas, civiles y criminales a la compañía o a sus Clientes. Está siempre restringida a un grupo específico de personas, pudiendo este estar compuesto por Clientes, Socios Comerciales, Accionistas/Dueños, Socios y/o Colaboradores. (ii) **Interna**, información de la compañía que la misma no quiere hacer pública y que el acceso de personas externas debe ser evitado. Si ocurriera que la información sea accedida de forma indebida, podrá causar daños a la imagen de la compañía, sin embargo, no con la misma magnitud de una información confidencial. Puede ser accedida sin restricciones por todos los Colaboradores y Socios Comerciales. (iii) **Información Pública**, información de la compañía o de sus Clientes con lenguaje y formato exclusivo para la divulgación al público en general, es de carácter informativo, comercial o promocional. Destinada al público externo o debido al cumplimiento de una ley vigente que exija publicidad de esta.

CSCH, además, asume el concepto de **Información Sensible** como aquella que puede afectar de forma importante la seguridad de las operaciones y activos de información de CSCH, siendo entonces su premisa la protección de la información relacionada con: (i) el proceso logístico involucrado en las importaciones, exportaciones y /o cadenas de suministro a su cargo, (ii) los sistemas internos, informáticos y/o de gestión, (iii) los procesos de vigilancia y acceso a las instalaciones, (iv) sus miembros, Clientes y Socios Comerciales, (vi) cualesquiera otros datos o información susceptibles de ser utilizados para fines ilícitos como el contrabando, narcotráfico, robo, legitimación de capitales, entre otros.

CSCH identifica los riesgos en función de su tamaño, su naturaleza y sus actividades, a fin de proteger la información relacionada con su gestión organizacional y con sus procesos comerciales, por lo que ha considerado como parte de su marco normativo de Seguridad de la Información y Protección de Datos, base para las Políticas, Normas y Procedimientos de la compañía, los quince numerales de capacidad operativa definidas en la norma ISO/IEC 27002:2022: (i) Gobernanza. (ii) Gestión de Activos. (iii) Protección de la Información. (iv) Seguridad en los Recursos Humanos. (v) Seguridad Física. (vi) Seguridad del Sistema y de la Red. (vii) Seguridad en Aplicaciones. (viii) Seguridad en la Configuración. (ix) Gestión de Identidad y Acceso. (x) Gestión de Amenazas y Vulnerabilidades. (xi) Continuidad. (xii) Seguridad en Relaciones con Proveedores. (xiii) Legal y Cumplimiento. (xiv) Gestión de Eventos de Seguridad de la Información. (xv) Aseguramiento de la Seguridad de la Información.

# POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION Y PROTECCION DE DATOS

## DATOS PERSONALES Y DATOS PERSONALES SENSIBLES

CSCH reconoce a los **Titulares de los Datos**, como las personas naturales a las que se refieren los datos de carácter personal; comprende los **Datos Personales**, como aquellos datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables y, los **Datos Personales Sensibles**, como aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y, la vida sexual. Asimismo, CSCH acepta la definición de **Responsable del Banco de Datos**, como la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos personales. CSCH, entiende, además, el **Tratamiento de Datos**, como cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

CSCH utilizará para la recolección de datos, formularios predeterminados que se entregan a los Titulares de Datos de forma digital para que estos los rellenen a través de los mecanismos físicos o digitales que ellos determinen, pero siempre serán devueltos por los Titulares de los Datos a CSCH de forma digital, luego de ser rellenados y firmados en señal de autorización. CSCH se asegura de que estos formularios contengan un apartado donde se solicita la autorización de los Titulares de los Datos para que CSCH realice el tratamiento de los datos recolectados, pero, aun así, CSCH entrega a los Titulares de los Datos un formato específico de Autorización para el Tratamiento de los Datos Personales. CSCH jamás solicitará a los Titulares de los Datos, la entrega de datos financieros a través de correos electrónicos.

Los Datos Personales y Datos Personales Sensibles recolectados por CSCH, serán utilizados únicamente para el cumplimiento del propósito del Tratamiento de Datos indicados en los formularios correspondientes y siempre dentro de las competencias y atribuciones de CSCH que, como Responsable del Banco de Datos, definan las autoridades chilena y extranjeras. En virtud de lo anterior, CSCH procura que en todos los formularios de recolección de datos que entrega a los Titulares de los Datos para ser rellenados, se informe sobre el Propósito del Tratamiento de Datos, no obstante y por regla general, el propósito del Tratamiento de Datos que CSCH dará a los datos recolectados será: (i) Almacenar y clasificar los Datos Personales para su fácil acceso e identificación; (ii) Analizar, procesar, evaluar y comparar información; (iii) Consultar, comparar y evaluar toda la información de Clientes, Socios Comerciales, Accionistas/Dueños, Socios y/o Colaboradores almacenados en bases de datos públicas judiciales y de seguridad, que permita establecer de manera integral el comportamiento de los mismos; (iv) Cumplir con la legislación chilena y extranjera, y con las órdenes judiciales o administrativas emitidas por las autoridades; (v) Proporcionar información a los reguladores y auditores internos o externos; (vi) Pagar o recibir pago y, determinar los impuestos locales y extranjeros; (vii) Cumplir con todas las obligaciones derivadas de la relación contractual entre CSCH y los Titulares de los Datos. Si en algún caso llegara a requerirse un tratamiento distinto de lo indicado deberá quedar registro del consentimiento/autorización del Titular de los Datos.

Los Titulares de los Datos tendrán derecho a autorizar o no la recolección y tratamiento de sus Datos Personales Sensibles por parte de CSCH y sus encargados. No obstante, si el Titular de los Datos no autoriza a CSCH a recolectar y hacer el tratamiento de estos Datos Personales Sensibles, CSCH no podrá cumplir con el Propósito del Tratamiento. De igual forma, CSCH podrá requerir transmitir los Datos Personales y Datos Personales Sensibles, a (i) compañías y filiales del mismo grupo corporativo de CSCH, incluso radicadas en diferentes jurisdicciones que no comparten niveles de protección de datos equivalentes a la legislación chilena, (ii) terceros a los que CSCH les encargue el Tratamiento de los Datos Personales y Datos

Personales Sensibles, los cuales siempre serán tratados bajo la responsabilidad de CSCH, en cumplimiento de esta Política de Seguridad de la Información y Protección de Datos y los más altos estándares de seguridad y confidencialidad aplicados por CSCH.

Los miembros de CSCH que en cualquier momento pudiesen interactuar con Datos Personales y Datos Personas Sensibles, están obligados a guardar secreto de estos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público; obligaciones que subsistirán indefinidamente, aún después de finalizar sus relaciones con CSCH.

Los datos entregados por sus titulares al utilizar el sitio web www.cschcs.com serán administrados exclusivamente por CSCH como Responsable del Banco de Datos, evitando usos indebidos u alteración, y serán almacenados únicamente durante el tiempo necesario para garantizar la prestación del servicio o el cumplimiento de la finalidad para la que fueron recolectados, sin perjuicio a las excepciones dispuestas en la Ley. Estos datos podrán ser conservados y tratados con fines estadísticos, siempre y cuando sea imposible la identificación de sus titulares. Si el Titular de los Datos, al usar el sitio web www.cschcs.com, se ha registrado para participar en un evento publicado en el sitio web, CSCH puede transferir su nombre, dirección de correo electrónico, número de teléfono y nombre de la empresa al organizador local y a los patrocinadores del evento con fines de marketing directo y para facilitar la preparativos y reservaciones para el evento; también, si ha expresado interés en comprar los productos o contratar nuestros servicios, CSCH puede transferir su nombre, dirección de correo electrónico, número de teléfono y nombre de la empresa a las otras unidades de negocio de grupo corporativo, para este propósito, de acuerdo a la logística de ejecución del servicio más adecuada. No obstante, a todo lo anterior, CSCH no se hará responsable del uso que puedan dar terceras personas a los Datos Personales entregados por sus titulares en espacios abiertos al público, como redes sociales o foros. En estos espacios públicos, que pueden estar asociados al sitio web www.cschcs.com, los datos serán almacenados junto al resto de contenidos, con el fin de permitir el funcionamiento, mantenimiento y transparencia de dichos sistemas y las contribuciones en él realizadas. En el link https://www.cschcs.com/privacy se puede leer completamente la Política de Privacidad y manejo de los datos recolectados a través de nuestro sitio web www.cschcs.com.

CSCH garantiza que todo Titular de los Datos podrá, en todo momento, ejercer los derechos otorgados por la Ley Nº 19.628 sobre protección de la vida privada, y sus modificaciones posteriores. Estos derechos son: (i) Exigir acceso a la información, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos; (ii) Que sus Datos Personales se modifiquen cuando sus registros sean erróneos, inexactos, equívocos o incompletos, y así se acredite; (iii) Exigir que se eliminen o bloqueen sus datos en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos, o cuando no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal; (iv) No obstante, no podrá solicitar acceso a la información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional. Tampoco podrá pedirse la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva; (v) El acceso a la información, modificación, eliminación o bloqueo de los datos serán absolutamente gratuitos, y no puede ser limitado por medio de ningún acto o convención; (vi) Efectuar reclamación ante la autoridad competente por infracciones a lo dispuesto en la ley aplicable; (vii) Revocar la autorización y/o solicitar la eliminación de su información personal cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o eliminación que se basen en esos supuestos, procederá cuando la autoridad competente haya determinado que CSCH ha incurrido en faltas contra la ley. Para garantizar a los Titulares de los Datos el ejercicio de estos derechos en cualquier

momento, CSCH establece un canal de comunicación específico a través del correo electrónico dataprotection@cschcs.com, pudiendo cambiar o establecer nuevos canales cuando así lo crea conveniente.

## RESPONSABILIDAD DE CUMPLIMIENTO

Cada miembro de CSCH, además de los Socios Comerciales y otros Socios, cuando corresponda, deben conocer, cumplir y hacer cumplir cabalmente las disposiciones de esta Política General de Seguridad de la Información y Protección de Datos, así como las demás Políticas, Normas y Procedimientos específicos que se deriven de ella.

Es responsabilidad de cada uno de los miembros de CSCH revisar y analizar las pautas de esta Política de Seguridad de la Información y Protección de Datos, regirse por ellas y contribuir dentro del ámbito de su trabajo a su ejecución.

La alta Gerencia de CSCH es responsable de apoyar el proceso de implementación de las Políticas de Seguridad de la Información y Protección de Datos, y asignar los recursos necesarios para su cumplimiento; también, verificar periódicamente, junto con cada Gerencia de Línea de la organización, el cumplimiento de las Políticas de Seguridad de la Información.

Las Gerencias de Línea son responsables de supervisar la implementación de la Política General de Seguridad de la Información y Protección de Datos, así como las demás Políticas, Normas y Procedimientos específicos que se deriven de ella; dar conocer sus contenidos a todo el personal a su cargo, así como exigirles constancia válida de haberse efectuado la lectura y entendimiento correspondiente, además de velar les den cumplimiento; revisar anualmente las Políticas, Normas y Procedimientos específicos derivados de esta política general, tanto por actualización y mejoras como por requerimiento de la Gerencia General en caso que se produzcan cambios significativos en la organización.

El incumplimiento de lo dispuesto en esta Política General podrá derivar en la aplicación de sanciones según corresponda y en conformidad con el mérito de cada situación, dando derecho a CSCH a ejercer las acciones civiles, penales y administrativas que correspondan, e incluso a proceder a la terminación de los contratos respectivos. Lo anterior, es sin perjuicio de la infracción que pudiera derivarse de lo dispuesto en la legislación y de la responsabilidad, de cualquier naturaleza, que en cada caso sea exigible.

## VIGENCIA

Esta Política General de Seguridad de la Información y Protección de Datos, y todo su contenido, tendrá vigencia a contar de su fecha de aprobación y puesta en marcha, y tendrá duración indefinida en tanto el Directorio o la Gerencia General no adopte otra resolución al respecto.

**Jorge Hurtado Indriago**
**CEO**