RESOLUCIÓN N° 10.475

Santiago, 20 de marzo de 2024.-

VISTO Y CONSIDERANDO

1) Que, Sercotec es una Corporación de Derecho Privado, cuya misión es ser la agencia de fomento productivo especializada en el apoyo a la micro y pequeña empresa y el emprendimiento en Chile, cuya acción experta, coordinada con los actores públicos y privados de los territorios, potencie los ecosistemas productivos, favoreciendo su desarrollo económico sostenible e inclusivo y un mayor bienestar para las personas.

2) Que, el Servicio de Cooperación Técnica requiere gestionar adecuadamente la Seguridad de la Información (SI) y Ciberseguridad, con objeto de mejorar niveles de protección de los activos de información en los procesos de provisión y soporte ante incidencias que pudieran afectar la normal continuidad de la operación, por lo que se hace necesario actualizar su Política de Seguridad de la Información.

3) Que, a través de la Resolución N°9850, de 04 de diciembre de 2019, de la Gerencia General de Sercotec, se aprobó la Política General de Seguridad de la Información del Servicio de Cooperación Técnica.

4) Las atribuciones conferidas por los Estatutos de Sercotec, particularmente lo señalado en la letra g, del artículo décimo cuarto, esta Gerencia General,

RESUELVE:

I. Déjase sin efecto la Resolución Interna N° 9850, de 04 de diciembre de 2019, de la Gerencia General de Sercotec, que aprobó la Política General de Seguridad de la Información del Servicio de Cooperación Técnica y sus posteriores modificaciones.

II. Apruébase la Política de Seguridad de la Información del Servicio de Cooperación Técnica, cuyo texto es el siguiente:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Servicio de Cooperación Técnica

1 INTRODUCCIÓN.

El Servicio de Cooperación Técnica (Sercotec) es consciente del crecimiento del uso e importancia de las Tecnologías de la Información (correo electrónico, Internet, redes de comunicaciones, computadores, periféricos, dispositivos móviles, extraíbles, entre otros), tanto en el ámbito personal como profesional, la necesidad de éstos como apoyo a las funciones del personal de Sercotec, considerando que los riesgos vinculados a los procesos de la institución estarán siempre presentes. Nuestro Servicio entiende que es imprescindible fijar las reglas que regulan su uso, a fin de evitar el impacto directo o indirecto que pudiese derivarse de su falta de regulación.

El presente documento constituye una política para la institución, destinada a normar los aspectos más relevantes de la gestión de Seguridad de la Información, con una vigencia de largo plazo, por lo cual se promulgarán documentos adicionales que explicitan en mayor detalle las medidas de seguridad dispuestas en la presente política.

Para que nuestra institución cuente con un sistema efectivo y eficiente respecto a la Seguridad de la Información y ciberseguridad, debe contar con una organización clara y plenamente establecida. Es esencial contar además con el conocimiento adecuado, definir los roles y responsabilidades, generar métricas y registros de aprendizaje de todos los integrantes de la institución e implementar procesos de mejora continua, lo que ayudará a establecer y de paso mejorar los ambientes de control de la Seguridad al interior de Sercotec.

En consecuencia, es necesario establecer **valores o principios** generales de seguridad de la información, que deben permanecer estables a través del tiempo, para el cumplimiento por parte de todos los trabajadores y colaboradores de Sercotec. Dichos valores son: **integridad, confidencialidad y disponibilidad.**

Considerando la importancia de cumplir con las disposiciones legales vigentes en materia de ciberseguridad y protección de datos, la presente política de seguridad de la información de Sercotec se enmarca en la Ley Nº 21.459, la cual establece normas sobre delitos informáticos y adecuación al Convenio de Budapest. Asimismo, se incorporan los lineamientos del Decreto N°164, de 2023, del Ministerio del Interior y Seguridad Pública, que aprueba política nacional de ciberseguridad 2023-2028, que regula la protección de datos personales y sensibles, garantizando la confidencialidad y privacidad de la información institucional. En este sentido, se designa al Director de Seguridad de la Información como responsable de velar por el cumplimiento de estas normativas y de implementar medidas de seguridad adecuadas para prevenir y gestionar incidentes de seguridad de la información.

Este documento constituye una política institucional destinada a normar los aspectos más relevantes de la gestión de Seguridad de la Información, con una visión de largo plazo. Adicionalmente, se emitirán documentos complementarios (normas, directrices, procedimientos,

instructivos, herramientas de seguridad etc.) para mitigar los riesgos asociados a la protección de activos de información, en concordancia con los definidos en la NCh-ISO 27000.

2 OBJETIVOS.

El propósito de la Política de Seguridad de la Información es mostrar en forma clara y sucinta la posición de Sercotec con respecto al buen uso de los **activos de información** corporativos.

Esto se traduce en:

a) Definir lineamientos o principios generales que sirven de medio para alcanzar los objetivos de la Seguridad de la Información.
b) Establecer responsabilidades aplicables a los distintos niveles jerárquicos y a todo el personal vinculado a Sercotec.
c) Fijar directrices sobre las cuales se sustenten normativas e instructivos de seguridad y ciberseguridad que desarrollen con mayor grado de detalle aspectos relativos a la seguridad de un tema particular o sistema en específico.
d) Definir medios de difusión al interior y exterior del Servicio para alineamiento con la Dirección.

Además, la presente Política, entrega directrices y recomendaciones que buscan establecer y consolidar las bases en que se sustentará **la cultura de Seguridad** en Sercotec.

3 ALCANCE.

La presente política establece un marco regulatorio aplicable a todo el personal que trabaja en las oficinas de Sercotec, ya sea sujeta a Código del Trabajo, dotación a honorarios, alumnos en práctica o externos que presten servicios permanentes o temporales; así como, proveedores, contratistas y personal que estén vinculados con las empresas que presten servicios en Sercotec o que estén relacionados, tanto a nivel central como regional.

También es aplicable a todo activo de información que la organización posea en la actualidad, asociados a los procesos del Servicio, de manera que la no inclusión explícita en el documento no constituye argumento para no proteger estos activos de información.

La política cubre toda la información, la impresa, la almacenada electrónicamente, la transmitida por correo o usando medios electrónicos, mostrada en video o hablada en una conversación, entre otras.

4 ROLES, RESPONSABILIDADES Y CUMPLIMIENTO.

4.1 Roles y responsabilidades.

4.1.1 Gerente General.

Para gestionar en forma adecuada la Seguridad de la Información al interior del Servicio de Cooperación Técnica, el Gerente General ocupa una posición de liderazgo clave y tiene

responsabilidades significativas en relación con la seguridad de la información dentro de la organización. Dentro de sus responsabilidades se encuentran las siguientes:

a) Debe demostrar un fuerte compromiso con la seguridad de la información y establecer un "tono desde la cima" que enfatice la importancia de la seguridad en toda la organización. Esto implica comunicar la importancia de proteger la información, cumplir con las políticas de seguridad y respaldar las iniciativas relacionadas con la seguridad.
b) Debe revisar y aprobar la política de seguridad de la información, asegurándose de que esté alineada con los objetivos y valores de la organización. Además, debe respaldar públicamente la política para que todo el personal de Sercotec, terceros que presten servicios a Sercotec y visitantes, comprendan su importancia.
c) Debe difundir, impulsar y apoyar la Seguridad de la Información y Ciberseguridad de Sercotec.
d) Debe asegurarse de que haya una colaboración efectiva entre las diferentes Gerencias, Direcciones Regionales y equipos en relación con la seguridad de la información.

4.1.2 Director de Seguridad de la Información.

Será el Gerente de Tecnología y Sistemas, o quien le subrogue, y será el principal responsable en la definición de los criterios de Seguridad de la Información y Ciberseguridad de Sercotec. Sus principales funciones son:

a) Liderar la estrategia Seguridad de la Información y Ciberseguridad de la institución siendo responsable de asegurar que sus objetivos sean establecidos, que sus requisitos se integren con los procesos de la institución, que los recursos necesarios estén disponibles, de comunicar sus requerimientos al personal de Sercotec, terceros que presten servicios a Sercotec y visitantes, de asegurar el logro de sus resultados esperados y de promover su mejora continua.
b) Dirigir y apoyar a las personas para que contribuyan a la eficacia de la Seguridad de la Información y Ciberseguridad.
c) Asegurarse de que el personal de Sercotec, terceros que presten servicios a Sercotec y visitantes, estén debidamente informados sobre las políticas y procedimientos de seguridad de la información. Esto incluye la implementación de programas de capacitación y concienciación para garantizar que comprendan sus responsabilidades en materia de seguridad.
d) Propiciar la existencia de mecanismos o procedimientos formales que permitan asegurar la continuidad del negocio ante situaciones que impidan el acceso a la información crítica para el funcionamiento de la institución.
e) Aprobar estructura de la seguridad de la información que contemple roles y responsabilidades.
f) Liderar la estrategia de Seguridad de la Información y Ciberseguridad al interior de Sercotec. Además, velar porque las distintas áreas del servicio implementen las políticas, procedimientos y controles relacionados con la Seguridad de la Información.
g) Sensibilizar a la Alta Dirección del servicio de los temas relevantes de la seguridad de la información.
h) Promover una cultura de seguridad en toda la organización, donde la protección de la información sea una responsabilidad compartida y se priorice en todas las actividades empresariales.

4.1.3 Encargado de Ciberseguridad.

Será designado por el Director de Seguridad de la Información y será la contraparte en materias de ciberseguridad. Sus principales funciones son:

a) Mantener y dar cumplimiento a un Plan Anual de Ciberseguridad.
b) Gestionar con los actores involucrados que se tomen acciones ante la ocurrencia de incidentes de ciberseguridad.
c) Coordinar internamente que se identifiquen amenazas y vulnerabilidades en términos de ciberseguridad.
d) Informar al Comité de Ciberseguridad sobre las medidas tomadas en el ámbito de la ciberseguridad.
e) Coordinar con el área de tecnología la adopción de medidas de ciberseguridad.
f) Reportar los incidentes de ciberseguridad al Equipo de Respuesta frente a Incidentes Informáticos del Estado (CSIRT).
g) Gestionar la ejecución de acciones preventivas en materia de ciberseguridad, incluyendo el mantenimiento de un plan de acción relacionado con la prevención de riesgos. Esta función será abordada por el especialista en ciberseguridad, quien también estará a cargo de mantener un plan de acción basado en los riesgos y/o brechas de seguridad de la información.

4.1.4 Especialista de Ciberseguridad.

Será designado por el Director de Seguridad de la Información, y trabará en conjunto con el Encargado de Ciberseguridad. Se debe centrar en la implementación, monitoreo y respuesta práctica a las amenazas cibernéticas. Su colaboración garantiza una defensa integral y eficiente contra los riesgos de seguridad y contribuye a la protección de la organización frente a las crecientes amenazas en el entorno digital. Dentro de sus responsabilidades deberá:

a) Entregar apoyo técnico y metodológico en materias de Ciberseguridad a la institución.
b) Realizar análisis de ciberseguridad.
c) Realizar análisis de riesgo considerando vulnerabilidades y amenazas de ciberseguridad.
d) Proponer medidas para mantener un nivel adecuado de ciberseguridad por medio del Plan Anual de Ciberseguridad.
e) Supervisar activamente los sistemas y redes en busca de actividad sospechosa o comportamientos anómalos que puedan indicar un ataque cibernético.
f) Cuando se detectan incidentes de seguridad, debe analizarlos para determinar la naturaleza y el alcance del ataque. Esto puede incluir la identificación de malware, la recopilación de evidencia y el seguimiento de patrones de actividad.
g) Es responsable de tomar medidas inmediatas para contener y mitigar los incidentes de seguridad.
h) Concientizar a la institución en materia de ciberseguridad.
i) Reportar los incidentes de ciberseguridad al CSIRT y al Encargado de Ciberseguridad de Sercotec.
j) Debe mantenerse actualizado sobre las últimas amenazas y tendencias en ciberseguridad.
k) Debe colaborar con otros equipos de TI, desarrolladores y responsables de diferentes áreas para garantizar que las prácticas de seguridad se integren de manera efectiva en todas las operaciones al interior de Sercotec.
l) Mantener y dar cumplimiento operativo a un Plan Anual de Ciberseguridad.

4.1.5 Comité de Ciberseguridad.

Órgano colegiado, cuya conformación, forma de funcionamiento y funciones específicas serán definidas por Resolución de la Gerencia General del Servicio, el cual asesorará al Gerente General en temas de Ciberseguridad, apoyará la implementación y procesos de mejoramiento de la Seguridad de la Información al interior del Servicio de Cooperación Técnica y será el responsable de la definición, implementación, difusión y mejora continua de las Políticas, Normas, Instructivos y cualquier otra documentación relacionada con la Ciberseguridad en Sercotec.

4.1.6 Personal de Sercotec.

Tiene la responsabilidad de cumplir con ésta y cada una de las políticas, normativas, procedimientos, instructivos, etc., que se definan para velar por la Seguridad de la Información y Ciberseguridad de Sercotec y aplicarlo en su entorno laboral.

4.1.7 Terceros que presten servicios a Sercotec.

En lo relativo a la información que obtengan a través de Sercotec, tienen la responsabilidad de cumplir con ésta y cada una de las políticas, normativas, procedimientos, instructivos, etc., que se definan para velar por la Seguridad de la Información y Ciberseguridad de Sercotec y aplicarlo en lo que sea pertinente. Además, tienen la obligación de alertar de manera oportuna y adecuada cualquier incidente que atente contra la seguridad de los activos de información de Sercotec, de acuerdo al procedimiento de registro de incidentes establecido para a estos fines.

4.1.8 Visitantes.

Deben observar y cumplir las exigencias relacionadas con la Seguridad de la Información, mientras se encuentra de paso por las instalaciones y oficinas del Servicio de Cooperación Técnica.

4.2 Cumplimiento.

El cumplimiento de esta política y procedimientos, u otros documentos que deriven de la Política General de Seguridad de la Información, deberá ser una tarea cotidiana y de estricta aplicación por parte de todo el personal de Sercotec, y en general de todos los colaboradores de la institución según lo establecido en el acápite “3. Alcance” de la presente política.

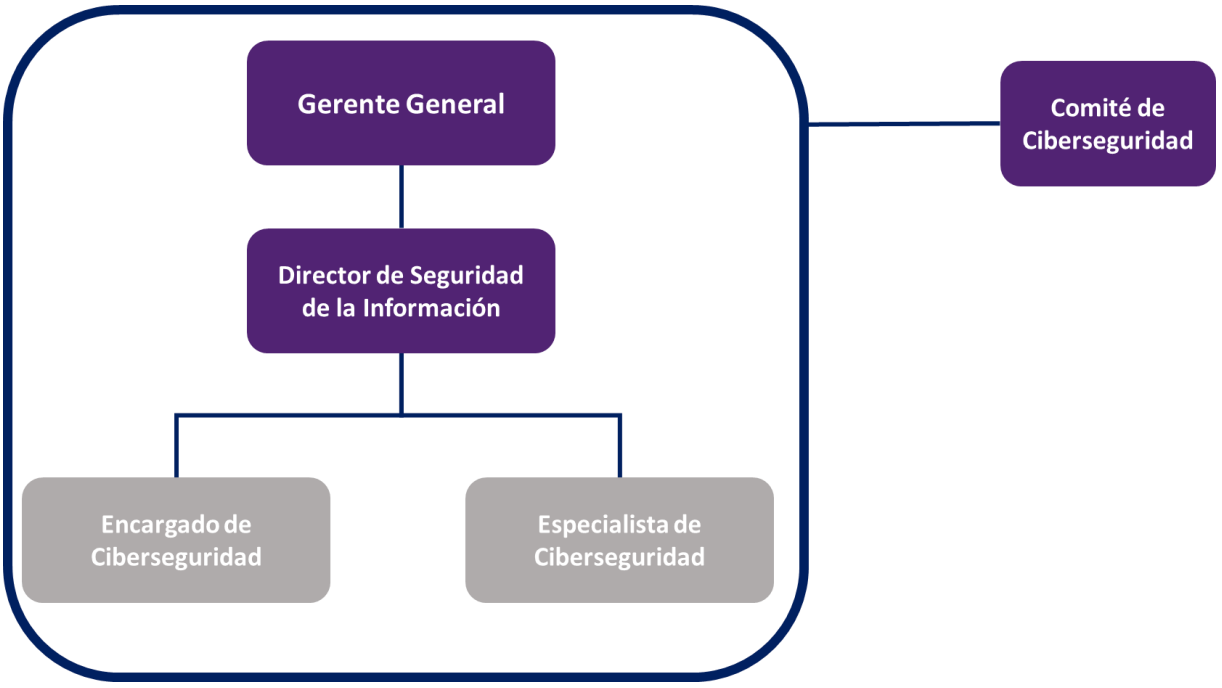
Ante cualquier incumplimiento o violación del contenido del presente documento y sus normas complementarias, ya sea parcial o total, el Director de Seguridad de la Información lo comunicará al Gerente General.

Es importante señalar que Sercotec ejercerá las acciones disciplinarias y legales, cuando corresponda, en contra de quienes no cumplan con lo estipulado en esta política, normativas, procedimientos y/o documentos que se desprendan de ella. Por lo tanto, Sercotec aplicará las sanciones establecidas en su Reglamento Interno de Orden, Higiene y Seguridad, para el caso de sus trabajadores y las sanciones establecidas en cada uno de los contratos, cuando corresponda a un tercero.

Con el fin de salvaguardar los activos de información institucionales, Sercotec deberá establecer y mantener un nivel apropiado de seguridad de la información para llevar a cabo sus actividades. Para esto Sercotec define una estructura con roles y responsabilidades para mantener un nivel adecuado

de seguridad. Además, se podrá basar en los controles establecidos por la norma ISO 27001 para mantener el nivel de seguridad de la información, implementando mediante políticas, planes, procedimientos, instructivos, registros y otros tipos de documentos que garanticen la protección adecuada del servicio en relación a la seguridad de la información.

5 ESTRUCTURA DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN.



6 DEFINICIONES.

a) **Activo de Información**: Se entenderá por activo de información todos aquellos elementos relevantes en la producción, emisión, comunicación, visualización y recuperación de información de valor estratégico para Sercotec, esto es:

- Los equipos y/o sistemas que soportan esta información.
- Las personas que utilizan la información y que tienen el conocimiento de los procesos institucionales del Servicio.

b) **Buen Uso**: Se entenderá por "buen uso" de los sistemas e información de Sercotec, el uso acorde a lo estipulado en las políticas, normas y procedimientos de la institución y en cualquier caso solo para propósitos relacionados con el servicio, a través del uso natural de los recursos.
Sercotec se reserva el derecho de tomar medidas administrativas para sancionar al personal en caso de existir evidencias de no cumplimiento o transgresión de lo establecido, sin perjuicio de la eventual responsabilidad civil y penal del mismo, tanto de sus funcionarios como de terceros.

c) **Confidencialidad**: Es asegurar que la información es accesible sólo para las personas autorizadas para ello. Todo el personal que trabaja en las oficinas de Sercotec, ya sea sujeta a

Código del Trabajo, dotación a honorarios, alumnos en práctica o externos que presten servicios permanentes o temporales; así como, proveedores, contratistas y personal que estén vinculados con las empresas que presten servicios en Sercotec o que estén relacionados, tanto a nivel central como regional deberán guardar confidencialidad respecto de la información a la que tenga acceso en el marco del ejercicio de sus funciones, o de aquella a la que tuviese acceso por error. Este deber puede ser relevado en los casos de autorización expresa de la jefatura respectiva y en los casos que se dé cumplimiento a las obligaciones impuestas por la Ley 20.285 sobre Acceso a la Información Pública.

d) **Datos de carácter personal o datos personales:** Los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

e) **Datos sensibles:** 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, la vida sexual entre otros.

f) **Disponibilidad**: Es asegurar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando estos sean requeridos.

g) **Director de Seguridad**: Es la persona que la autoridad máxima del Servicio designa para la definición, diseño, implementación y supervisión de las medidas de Seguridad de la Información y Ciberseguridad.

h) **Incidente de Seguridad:** Es un hecho consumado, de forma intencional o no intencional que ha afectado la confidencialidad, integridad o disponibilidad a los activos y/o sistemas de información de Sercotec, y sobre los cuales deben tomarse medidas correctivas inmediatas con el objeto de evitar daños mayores o reincidencias.

i) **Información**: Es toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

j) **Integridad**: Es salvaguardar la exactitud y totalidad de la información en su procesamiento, transmisión y almacenamiento.

k) **Personal:** Personas naturales que presten servicios para Sercotec sujetos a Código del Trabajo o a Honorarios, a las cuales se le concede autorización para acceder a la información y a los sistemas de Sercotec. El personal puede ser interno o externo a la institución.

l) **Seguridad de la Información**: Se entenderá como Seguridad de la Información, el establecimiento de un sistema que incluye diversos controles que garantizan que los activos de información cumplan con adecuados niveles de integridad, confidencialidad y disponibilidad, frente a posibles amenazas que puedan poner en riesgo la continuidad del negocio.

m) **Ciberseguridad:** La Ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos en el ciberespacio.

n) **Terceros:** Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, estudiantes en práctica, que provean servicios o productos a la Organización a los cuales se le concede autorización para acceder a la información y a los sistemas de Sercotec.

7 POLÍTICA.

7.1 Enunciado de la política

Sercotec reconoce la información como un activo clave, por lo que asume la responsabilidad de velar por Seguridad de la Información y Ciberseguridad para que preserve niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucionales.

7.2 De la información interna.

a) La información es un activo vital, por lo que su utilización, es decir, accesos, procesamiento y mantenimiento deberán ser consistentes con lo instruido en las políticas, normas, y procedimientos emitidos por Sercotec en cada ámbito en particular.

b) La información debe ser protegida, por sus custodios, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas específicas de seguridad de la información o sus procedimientos asociados y en las recomendaciones dadas por el responsable designado de dicha información.

c) Toda información creada o procesada por la institución debe ser considerada como "pública", a menos que se determine expresamente lo contrario. Sercotec proveerá los mecanismos para que la información sea accedida y utilizada por el personal que de acuerdo a sus funciones así lo requiera. Sin embargo, se reserva el derecho de revocar al personal, el privilegio de acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameriten. Y, así mismo, una vez egresado del Servicio las obligaciones de confidencialidad de información estarán reguladas en el procedimiento de egreso de Sercotec.

7.3 De la información de los usuarios externos.

a) Si la institución procesa y mantiene información de usuarios externos que sean datos personales y/o sensibles de acuerdo a la normativa vigente, la institución se compromete a asegurar que esta información no será divulgada sin previa autorización y estará protegida de igual manera que la información interna, de conformidad a lo establecido en la Ley N° 19.628, sobre protección de la vida privada, sin perjuicio de lo señalado en la Ley N° 20.285.

b) En el caso de información de usuarios externos que se procese y mantenga, y que no tenga las características anteriormente mencionadas, ésta podrá ser divulgada sin previa autorización.

c) Si se requiere compartir información de los usuarios externos de Sercotec con instituciones externas, con motivo de externalizar servicios, a éstas se les exigirá un contrato, cláusula de confidencialidad y no divulgación de la información y/o convenio de transferencia de datos personales.

7.4 De la Auditorías.

Con el fin de velar por el correcto uso de los activos de información, Sercotec podrá realizar revisiones y/o auditorias en cualquier momento el cumplimiento de la política y documentos vigentes que digan relación con el acceso y uso que los usuarios hacen de los activos de información. Las auditorías podrán ser realizadas internamente, a través de Unidad de Auditoría Interna, o por auditorías a cargo de organizaciones externas, cuando sea pertinente y requerido por el Director de Seguridad de la Información.

7.5 Gestión de Incidentes y Continuidad del Negocio.

En el marco de la gestión integral de la seguridad de la información y ciberseguridad en Sercotec, se reconoce la importancia de contar con un Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones. Este plan, diseñado para garantizar la disponibilidad y continuidad de los servicios de tecnología de la información en situaciones de crisis o incidentes, se alinea estrechamente con los principios y objetivos establecidos en la presente Política de Seguridad de la Información.

El Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones de Sercotec incluye medidas específicas para la identificación de riesgos, la respuesta a incidentes, la recuperación de sistemas y datos, así como la comunicación interna y externa en caso de contingencias. Este plan se integra como parte fundamental de las acciones preventivas y correctivas destinadas a proteger los activos de información de la institución y garantizar la continuidad operativa en escenarios adversos.

7.6 De la gestión de la seguridad de la información y ciberseguridad.

La Seguridad de la Información y Ciberseguridad debe ser aplicada en lo posible a los procesos de negocio críticos o relevantes de la institución.

Los documentos relacionados a la Seguridad de la Información deberán ser validados por el Director de Seguridad de la Información.

El cumplimiento de los objetivos de seguridad de la información y ciberseguridad de Sercotec se basarán en realizar acciones que mantengan un nivel de seguridad adecuado para la prestación de los servicios. Dentro de las actividades que se pueden realizar, se consideran las siguientes:

i. Identificar y clasificar los activos de información involucrados más relevantes.
ii. Analizar el riesgo de ciberseguridad.
iii. Plan de Trabajo de Ciberseguridad.
iv. Mantener políticas y procedimientos u otro tipo de documento para generar un ambiente controlado de seguridad.
v. Difundir al personal de Sercotec, terceros que presten servicios a Sercotec y visitantes, el objetivo corporativo de la preservación de la información y ciberseguridad, sus características y las responsabilidades individuales para lograrlo.
vi. Implementar un sistema de gestión de la capacitación y concientización en seguridad de la información y la ciberseguridad.

7.7 Deberes del personal y de los terceros.

a) La información y las tecnologías de información deben ser usadas sólo para propósitos relacionados con el Servicio y autorizados por la jefatura directa, para el personal y la contraparte técnica de la respectiva contratación, para el caso de los terceros, debiéndose aplicar criterios de buen uso.
b) Las claves de acceso a la información y a las tecnologías de información son individuales, intransferibles y de responsabilidad única de su propietario.
c) El personal y los terceros están en la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política según procedimientos que se establezcan en el manejo de incidentes.
d) Se prohíbe la divulgación de información que esté considerada o clasificada como "reservada".

7.8 Organización de la Seguridad.

Con el objetivo de garantizar el cumplimiento de la Política General de Seguridad de la Información y las políticas específicas que se definan posteriormente, Sercotec ha establecido una estructura organizacional de Seguridad y Ciberseguridad que contempla la definición de funciones específicas en el ámbito de Seguridad y Ciberseguridad definidas en esta política, las cuales serán ejecutadas por un Comité de Ciberseguridad, un Director de Seguridad, un Encargado de Ciberseguridad y un Especialista de Ciberseguridad.

7.9 Revisión de la Política.

La revisión y/o reevaluación de la Política General de la Seguridad de la Información deberá realizarse por lo menos una vez cada dos años o, ante cualquier cambio significativo de tecnología, personal o evento que amerite su reevaluación para asegurar continuidad, idoneidad, eficiencia y efectividad. Esto lo debe realizar el Director de Seguridad de la Información.

7.10 Difusión de la Política.

La presente política será difundida al personal de Sercotec, terceros que presten servicios a Sercotec y visitantes, a través de la publicación en la Intranet institucional y en los respectivos contratos.

8 DOCUMENTACIÓN DE REFERENCIA.

Se considerará como documentación de referencia para la presente política, toda la normativa vigente, en particular:

- Decreto Supremo Nº 83 de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Ley N° 17.336, sobre Propiedad Intelectual.
- Ley N° 21.459 que establece normas sobre delitos informáticos, deroga la ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.
- Ley N° 19.628, sobre Protección de la Vida Privada.
- Ley N° 20.285, de transparencia de la función pública y de acceso a la información de la Administración del Estado.

- Ley N° 19.799 Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Decreto N°273, de 2022, del Ministerio del Interior y Seguridad Pública, que establece obligación de reportar incidentes de ciberseguridad.
- Decreto N°164, de 2023, del Ministerio del Interior y Seguridad Pública, que aprueba política nacional de ciberseguridad 2023-2028.
- Norma NCh- ISO 27001.
- Norma NCh- ISO 27002.
- Norma técnica sobre fundamentos generales de ciberseguridad para el diseño, instalación y operación de redes y sistemas utilizados para la prestación de servicios de telecomunicaciones. de la Subsecretaría de Telecomunicaciones.

COMUNÍQUESE

MARÍA JOSÉ BECERRA MORO
GERENTA GENERAL
SERCOTEC

JCLA/IQB/SCV
Distribución:
A todo Sercotec

REVISIONES DEL DOCUMENTO		
Código documento: P-SEG-01		
Versión	**Fecha Aprobación**	**Resumen de Modificaciones**
1.0	03- 2011	Creación del documento Sercotec.
2.0	11-2014	Revisión crítica de primera versión e inclusión de secciones faltantes.
3.0	07- 2016	Revisión crítica de versión anterior y modificación de todas las secciones de documento Política (consultora Ingenia).
4.0	07-2018	Revisión crítica de versión anterior: se corrige, actualiza y completa historial de revisiones, se modifica por completo la sección “Política”, resumiendo su desarrollo: se extrae el detalle extenso que implica la descripción de los ámbitos de seguridad y se incorporan contenidos en relación al marco de trabajo general para la gestión de la seguridad de la información. Se complementa información en sección Responsabilidades y Cumplimiento.

REVISIONES DEL DOCUMENTO		
Código documento: P-SEG-01		
Versión	**Fecha Aprobación**	**Resumen de Modificaciones**
5.0	12- 2018	Se delimita el alcance de la Política a los procesos críticos de negocio de Sercotec
6.0	11-2019	Se actualiza según nueva definición de estructura de la seguridad de la información
7.0	03-2024	Se actualiza estructura de la seguridad de la información y ciberseguridad Se elimina lo definido para el PMG de seguridad de la información Se actualizan elementos de política reflejando el foco existente en ciberseguridad y eliminando lo relativo a PMG.

CONTROLES APLICABLES PARA ESTA POLÍTICA	
Control	**Descripción**
A.5.1.1	Políticas para la seguridad de la información
A.5.1.2	Revisión de las políticas de seguridad de la información

SC I CLA AF

Maria José Becerra Moro
GERENTA GENERAL
SERVICIO DE COOPERACION TECNICA

FIRMADO ELECTRONICAMENTE EN FEBRERO