



## RESOLUCIÓN N° 9850.

SANTIAGO, 04 de diciembre de 2019.

### VISTO Y CONSIDERANDO:

- 1.- La necesidad del Servicio de Cooperación Técnica de gestionar adecuadamente la Seguridad de la Información (SI), 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.
- 2.- La Resolución N°9693, de 14 de diciembre de 2018, que aprobó la Política General de Seguridad de la Información del Servicio de Cooperación Técnica.
- 3.- La Resolución N°9697, de 28 de diciembre de 2018, que rectificó la Política General de Seguridad de la Información del Servicio de Cooperación Técnica.
- 4.- Que, en base al mejoramiento continuo del sistema de seguridad de la información se efectuó una revisión por parte del Comité de Seguridad de la Información en sesión del lunes 25 de noviembre del 2019 y se acordó modificar la Política General de Seguridad de la Información según consta en el Acta N°4.
- 5.- Las atribuciones conferidas por los Estatutos de Sercotec, particularmente lo señalado en la letra g, del artículo décimo cuarto, esta Gerencia General,

**RESUELVE:**

I. A contar de esta fecha se deja sin efecto la Resolución Interna N° 9693, de 14 de diciembre de 2018, 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 General de Seguridad de la Información del Servicio de Cooperación Técnica, cuyo texto es el siguiente:

---

# **POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN**

## **Servicio de Cooperación Técnica**

---



## TABLA DE CONTENIDOS

1	INTRODUCCIÓN.....	5
2	OBJETIVOS.....	6
3	ALCANCE.....	6
4	RESPONSABILIDADES Y CUMPLIMIENTO.....	6
4.1	RESPONSABILIDADES.....	6
4.2	CUMPLIMIENTO.....	8
5	DEFINICIONES.....	9
6	POLÍTICA.....	10
6.1	ENUNCIADO DE LA POLÍTICA.....	10
6.2	DE LA INFORMACIÓN INTERNA.....	10
6.3	DE LA INFORMACIÓN DE LOS USUARIOS EXTERNOS.....	11
6.4	DE LA AUDITORÍAS.....	11
6.5	DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.....	11
6.6	DEBERES DEL PERSONAL Y DE LOS TERCEROS.....	12
6.7	ORGANIZACIÓN DE LA SEGURIDAD.....	12
6.8	REVISIÓN DE LA POLÍTICA.....	13
6.9	DIFUSIÓN DE LA POLÍTICA.....	13
7	DOCUMENTACIÓN DE REFERENCIA.....	13



### REVISIONES DEL DOCUMENTO

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.
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

### 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

	<b>SERVICIO DE COOPERACIÓN TÉCNICA SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: P-SEG-01 Fecha: 28/11/19 Versión: 6.0 Página: 5 de 13
	<b>POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN</b>	

## 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. Nuestra institución 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.

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.**

Esta Política General de Seguridad de la Información, se encuentra basada en la Norma NCH-ISO 27001, y en lo establecido en el Decreto Supremo N° 83 de 2004, del Ministerio Secretaría General de la Presidencia.

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.

Dichas materias adicionales (normas, directrices, procedimientos, instructivos, herramientas de seguridad etc.) permitirán mitigar los riesgos que pudiesen afectar la protección de activos de información y deberán estar asociados a los dominios definidos en la NCh-ISO 27001:2013. Estos son:

- a) Política de seguridad de la información.
- b) Gestión y organización de la seguridad de la información.
- c) Seguridad de los recursos humanos.
- d) Gestión de activos.
- e) Control de acceso.
- f) Criptografía.
- g) Seguridad física y del ambiente.
- h) Seguridad de las operaciones.
- i) Seguridad de las comunicaciones.
- j) Adquisición, desarrollo y mantenimiento de los sistemas de información.
- k) Relaciones con el proveedor.
- l) Gestión de incidentes en la seguridad de la información.
- m) Aspectos de la seguridad de la información en la gestión de la continuidad del negocio.
- n) Cumplimiento.

	<b>SERVICIO DE COOPERACIÓN TÉCNICA SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: P-SEG-01 Fecha: 28/11/19 Versión: 6.0 Página: 6 de 13
	<b>POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN</b>	

## 2 OBJETIVOS.

El propósito de la Política General 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 un Sistema de 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 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.
- e) Definir plazos y periodicidad para su revisión y evaluación de cumplimiento.

## 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 de SERCOTEC, 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, entre otras, la impresa, la almacenada electrónicamente, la transmitida por correo o usando medios electrónicos, mostrada en video o hablada en una conversación, entre otras.

## 4 RESPONSABILIDADES Y CUMPLIMIENTO.

### 4.1 Responsabilidades.

- a) **Gerente General:** En su calidad de tal, es responsable de difundir, impulsar y apoyar el desarrollo de un adecuado Sistema de Gestión en Seguridad de la Información, como asimismo de la aprobación de la Política General de Seguridad de la Información y sus modificaciones, las que serán aprobadas a través de resolución.

	<b>SERVICIO DE COOPERACIÓN TÉCNICA SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: P-SEG-01 Fecha: 28/11/19 Versión: 6.0 Página: 7 de 13
	<b>POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN</b>	

- b) **Director de Seguridad de la Información:** Es el principal responsable en la definición de los criterios de seguridad de la información de Sercotec y sus principales funciones son:
- i) Liderar la estrategia del sistema de gestión de seguridad de la información 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 a los colaboradores, de asegurar el logro de sus resultados esperados y de promover su mejora continua.
  - ii) Dirigir y apoyar a las personas para que contribuyan a la eficacia del sistema de gestión de seguridad de la información.
  - iii) Velar por la existencia de un plan formal de difusión de la política de seguridad de la información y los documentos específicos que la sustenten.
  - iv) Velar que todo el personal reciba entrenamiento necesario en materia de seguridad de la información, consistente con sus necesidades y su rol dentro de Sercotec.
  - v) 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.
  - vi) Sensibilizar a la dirección acerca de la estrategia y los avances de la implementación del sistema de gestión de seguridad de la información institucional y del PMG y del cumplimiento de las metas y objetivos establecidos en el marco del Programa de Mejoramiento de la gestión PMG.
- c) **Encargado de Seguridad de la información:** Es quien realiza seguimiento a la implementación del SGSI y sus controles, y reporta a las partes interesadas de la institución respecto de la seguridad de la Información. Dentro de sus principales funciones se encuentra:
- i) Velar por el correcto y oportuno cumplimiento de los requisitos técnicos del indicador de Seguridad de la Información establecidos en el Programa Marco del PMG.
  - ii) Controlar periódicamente los avances del indicador de Seguridad de la Información, velando por la correcta emisión de los medios de verificación.
  - iii) Reportar los avances del indicador a la Unidad de Gestión Estratégica, comité de Seguridad de la Información y al Director de Seguridad de la Información.
  - iv) Controlar a los encargados de controles de la seguridad de la información en su implementación y mantenimiento.
  - v) Gestionar y planificar las auditorías internas para validar el funcionamiento del Sistema de Seguridad de la Información.
  - vi) Planificar y dirigir reuniones del Comité de Seguridad de la Información, elaborar presentaciones, actas y seguimiento a compromisos.
  - vii) Llevar el control de los incidentes de seguridad y las acciones correctivas y preventivas pertinentes cuando ocurran eventos e incidentes de seguridad de la información e informar a las partes interesadas.

	<b>SERVICIO DE COOPERACIÓN TÉCNICA SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: P-SEG-01 Fecha: 28/11/19 Versión: 6.0 Página: 8 de 13
	<b>POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN</b>	

viii) Planificar y dirigir las actividades de sensibilización, difusión y capacitación de Seguridad de la Información y evaluar sus resultados.

- d) **Comité de Seguridad de la Información:** tiene por responsabilidad asesorar al Gerente General, en temas de seguridad de la información, en coordinación con el Director de Seguridad. Su integración y funcionamiento será regulado por Resolución de Gerencia General.
- e) **Personal de Sercotec:** tiene la responsabilidad de cumplir con ésta y cada una de las políticas, normativas, procedimientos, instructivos, etc., que se definan en el Sistema de Gestión de Seguridad de la Información de Sercotec y aplicarlo en su entorno laboral. 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.
- f) **Terceros:** 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 en el Sistema de Gestión de Seguridad de la Información de Sercotec y aplicarlo en su entorno laboral. 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.

#### 4.2 Cumplimiento.

El cumplimiento de esta política general, políticas específicas 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.

	<b>SERVICIO DE COOPERACIÓN TÉCNICA</b> <b>SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: P-SEG-01 Fecha: 28/11/19 Versión: 6.0 Página: 9 de 13
	<b>POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN</b>	

## 5 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) **Comité de Seguridad:** es el equipo conformado por representantes de las áreas de la institución responsables de la toma de decisiones en temas de seguridad de la información.
- d) **Confidencialidad:** Es asegurar que la información es accesible sólo para las personas autorizadas para ello.
- e) **Datos de carácter personal o datos personales:** los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.
- f) **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.
- g) **Disponibilidad:** Es asegurar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando estos sean requeridos.
- h) **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.
- i) **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.

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

## 6 POLÍTICA.

### 6.1. Enunciado de la política.

Sercotec reconoce la información como un activo clave, por lo que asume la responsabilidad de implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) que preserve niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucionales.

### 6.2. 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, sus procedimientos asociados

	<b>SERVICIO DE COOPERACIÓN TÉCNICA SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: P-SEG-01 Fecha: 28/11/19 Versión: 6.0 Página: 11 de 13
	<b>POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN</b>	

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.

### **6.3. 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 a 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

### **6.4. De la Auditorías.**

Con el fin de velar por el correcto uso de los activos de información, Sercotec se reserva el derecho de auditar en cualquier momento el cumplimiento de las políticas 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 Encargado de Seguridad en coordinación con el Comité de Seguridad de la Información.

### **6.5. De la gestión de la seguridad de la información.**

La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado y conocido por la institución. Este proceso de gestión deberá ser aplicado a los procesos de negocio críticos de la institución.

	<b>SERVICIO DE COOPERACIÓN TÉCNICA SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: P-SEG-01 Fecha: 28/11/19 Versión: 6.0 Página: 12 de 13
	<b>POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN</b>	

Todos los documentos relacionados a la seguridad de la información deberán ser revisados por el encargado de seguridad de la información y aprobados por el Director de Seguridad de la Información.

El cumplimiento de los objetivos del SGSI de Sercotec se basará en la identificación de los activos de información involucrados en los procesos de negocio críticos, lo que implica a toda la estructura definida para la de la Seguridad de la Información, junto a los responsables de los diferentes procesos y subprocesos de negocio de Sercotec realizar las siguientes actividades fundamentales:

- i. Identificar y clasificar los activos de información involucrados.
- ii. Para cada activo de información, identificar un responsable.
- iii. Analizar el riesgo al cual están expuestos.
- iv. Difundir en forma planificada entre todo el personal de la institución el objetivo corporativo de la preservación de la información, sus características y las responsabilidades individuales para lograrlo, inserto esto, en planes de capacitación anual de la institución como actividades permanentes y en el proceso de inducción del nuevo personal.

#### **6.6. 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, 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 está 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".

#### **6.7. 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 que contempla la definición de funciones específicas en el ámbito de seguridad, las cuales serán ejecutadas por un comité de seguridad, un director de seguridad, un encargado de seguridad, un encargado de ciberseguridad y encargados de controles de seguridad de la información.

Las características de esta instancia organizacional y roles se detallan en la política específica de gestión y organización de la seguridad de la información que el Servicio establezca.

	<b>SERVICIO DE COOPERACIÓN TÉCNICA</b> <b>SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: P-SEG-01 Fecha: 28/11/19 Versión: 6.0 Página: 13 de 13
	<b>POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN</b>	

### 6.8. 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 Encargado de Seguridad de la Información en conjunto con el Director de Seguridad de la Información.

### 6.9. Difusión de la Política.

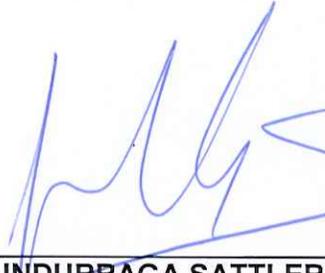
La presente política será difundida a todo el personal de Sercotec a través de la publicación en la intranet, así como por correo electrónico institucional.

## 7 DOCUMENTACIÓN DE REFERENCIA.

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

- Decreto Supremo N° 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° 19.223 que tipifica figuras penales relativas a la informática.
- Ley N° 19.628, sobre protección a la vida privada.
- Ley N° 20.285, Sobre acceso a la información pública.
- Ley N° 19.799 Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Norma NCh- ISO 27001:2013.
- Norma NCh- ISO 27002:2013.

### III. COMUNÍQUESE

  
**CAROLINA UNDURRAGA SATTLER**  
**GERENTE GENERAL**  
**SERCOTEC**



FCM/CFC/ JCLA/JSQ  
 Distribución:  
 A todo Sercotec