FUNDACIÓN
PAZ CIUDADANA
Políticas públicas en seguridad y justicia

Política Seguridad de la Información

FUNDACIÓN PAZ CIUDADANA

VERSIÓN: 2.0	FECHA: 15.07.2025	AUTORIZACIÓN		
		PREPARÓ Priscilla Schmidt	APROBÓ Priscilla Schmidt	APROBÓ Daniel Johnson

Contenido

1. Antecedentes.

Fundación Paz Ciudadana ha ido incorporando dentro de sus actividades relacionadas a la realización de estudios y a la implementación de programas, el uso de datos de carácter cualitativo y cuantitativo, que en la actualidad constituyen un insumo relevante para la generación de políticas públicas en materia de prevención y seguridad ciudadana, que inspira el actuar institucional. Por tanto, dado que para la Fundación los datos constituyen un bien estratégico, es necesario garantizar su protección en los procesos de obtención, procesamiento, transmisión y almacenamiento.

Este documento busca velar por la confidencialidad, integridad y disponibilidad de los datos, siempre dentro de los marcos normativos vigentes.

2. Objetivos y alcances de la política de seguridad de la información

2.1 Objetivos de la política de seguridad de la información.

a. Establecer normas que regulen el uso y manejo de los activos de información de la Fundación a través de las distintas actividades que el personal de la institución realiza en el desempeño de sus funciones, con el fin de asegurar la confidencialidad, integridad y disponibilidad de esta.

b. Establecer requisitos y condiciones generales de protección y resguardo de la seguridad de la información a las que se encuentra sujeta la institución de acuerdo a las normas legales pertinentes, así como los riesgos a que están expuestos sus activos de información y los principios y objetivos internos para el resguardo de sus operaciones.

2.2 Alcances de esta política.

La seguridad de la información es de responsabilidad de la totalidad de las personas que tengan acceso a los activos de información de la institución, sean personas que tienen un contrato de trabajo indefinido, a plazo fijo o a honorarios con la Fundación, personas que realizan asesorías, consultorías o prácticas profesionales con la Fundación o cualquier otra persona natural o jurídica que preste servicios a la Fundación y tenga acceso a dichos activos. Por ello, esta política es de conocimiento y cumplimiento obligatorio para toda persona a la que se le otorgue acceso a los activos de información institucionales.

La obligación antes referida deberá expresarse en los contratos o documentos en que se formalice la relación contractual entre la Fundación y dichas personas.

Asimismo, esta política es aplicable a todo activo de información que la organización posea actualmente o en el futuro, cubriendo prioritariamente aquellos activos asociados a la actividad principal de Fundación Paz Ciudadana.

3. Glosarios de términos

Activo de información: todo elemento en que se registre, almacene y/o procese datos e información a través de medios tecnológicos y otros soportes tales como bases de datos, archivos, contratos, acuerdos, documentación de sistemas, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, planes de continuidad operativa, información de auditorías, información archivada, activos de software, activos físicos como salas de computación, computadores y servidores, impresoras y redes de comunicación y servicios.

Confidencialidad: situación consistente que la información no esté disponible ni pueda ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: propiedad de la información que la hace ser accesible y utilizable por solicitud de una entidad autorizada.

Incidente de seguridad de la información: evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de un servicio o actividad y/o amenazar la seguridad de la información.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Sistema de gestión de seguridad de la información: parte del sistema de gestión basada en un enfoque hacia los riesgos de un negocio, cuyo fin es establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

4. Roles y cargos relacionados a la seguridad de la información

4.1 Los siguientes roles y cargos tienen responsabilidad en la administración y gestión de la política de seguridad de la información:

- Dirección Ejecutiva
- Encargado de Seguridad de la Información

4.2 La dirección ejecutiva, en su calidad de representante legal de Fundación Paz Ciudadana, le corresponde la aprobación de esta política y de sus futuras modificaciones. Además, velará por su cumplimiento y podrá delegar estas atribuciones en la Gerencia de Administración y Finanzas.

4.3 El Encargado de Seguridad de la Información tendrá a su cargo el desarrollo de las políticas de seguridad y el control de su implementación. Deberá además velar por su correcta aplicación y periódica actualización. Asimismo, deberá coordinar la respuesta a incidentes de seguridad de la información.

4.4 El rol de Encargado de Seguridad de la Información le corresponderá al Director del área de Datos e Investigación Aplicada vigente.

5. De la gestión de la seguridad de la información

5.1 La gestión de seguridad de la información deberá siempre mantenerse dentro de los ámbitos señalados por las normas legales y reglamentarias correspondientes.

5.2 En el caso de datos gestionados en Chile, dicho marco normativo corresponde al menos a las siguientes normas, aunque incluyen cualquier otra norma de rango legal o reglamentario aplicable a la materia y las modificaciones futuras de las que actualmente existieren

- Ley 17.336 de propiedad intelectual
- Ley 19.628 sobre protección de la vida privada
- Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de dicha firma
- Ley 20.285 sobre acceso a la información pública
- Ley 21.459 que establece normas sobre delitos informáticos.

5.3 En el caso de datos gestionados desde Chile, pero obtenidos en el extranjero, regirán los marcos normativos de los países donde estos se hayan obtenido.

5.4 La responsabilidad en el manejo de los activos de información de la institución recae en todas las personas señaladas en la sección 2.2 antes descrita, quienes deben hacer uso de los mismos en la forma autorizada y en directa y exclusiva relación con las funciones que desempeñan y, en consecuencia, con la normativa legal vigente.

5.5 Asimismo es obligación de estas personas reportar cualquier situación o evento que pueda exponer o afectar la integridad, confidencialidad o disponibilidad de los activos de información. Este reporte debe hacerse tan pronto como se tome conocimiento de dicha situación al Encargado de Seguridad de la Información. De dicha comunicación deberá dejarse respaldo dentro de las 24 horas siguientes vía correo electrónico, con copia a la jefatura directa.

5.6 La Fundación podrá establecer reglas especiales y más estrictas para la gestión de datos con contrapartes determinadas en el contexto de proyectos particulares. En tal caso, dichas reglas deberán constar por escrito en el convenio o contrato donde las partes regulen sus obligaciones reciprocas. En caso de que la Fundación se obligue en dichos actos a respetar determinados protocolos, políticas o normas en materia de gestión de datos, deberá estarse a lo que dichas regulaciones indiquen en la materia.

5.7 La difusión de la presente política, los procedimientos y otros documentos, se efectuará a través de los canales de difusión oficiales establecidos, pudiendo utilizarse publicación en la intranet institucional y/o correo electrónico u otro medio que la Fundación considere pertinente.

6. Acciones disciplinarias

El incumplimiento de esta Política por parte de colaboradores internos o externos será considerado una falta grave y podrá dar lugar a la aplicación de medidas correctivas o sancionatorias, de acuerdo con la normativa laboral vigente, los

contratos suscritos, y las políticas internas de la Fundación. Las medidas aplicables podrán incluir, sin limitarse a:

- Amonestaciones verbales o escritas (en el caso de personal interno).
- Restricción o suspensión de acceso a sistemas y recursos de información.
- Terminación del vínculo laboral o contractual, conforme a las disposiciones legales o contractuales aplicables.
- Acciones legales por perjuicios ocasionados, uso indebido de información o violación de la confidencialidad.

La severidad de la medida dependerá de la naturaleza y gravedad de la infracción, su impacto en la seguridad de la información, la reiteración de conductas y la intencionalidad del acto.

El personal externo que acceda a los sistemas, instalaciones o datos de la Fundación deberá conocer y adherir expresamente a esta política como condición para prestar servicios.

7. Vigencia de la presente política

Las disposiciones acá descritas comenzaran a regir a partir del 1 de julio de 2025.