Sisener
futuro sostenible

POLÍTICA DE SEGURIDAD DE LA INFORMACION

1. INTRODUCCIÓN

GRUPO SISENER velará por la protección de la información, independientemente de la forma en la que esta se comunique, comparta, proyecte o almacene (en adelante, la "Información"). Esta protección afecta tanto a la información existente dentro del Grupo como a la información compartida con terceros.

En este sentido, se entiende por Seguridad de la Información, la salvaguarda y protección de (i) la Información titularidad del Grupo, con independencia de que se encuentre en sistemas propios o de terceros; y (ii) la información titularidad de terceros, que se encuentre en sistemas del Grupo.

A los efectos de la presente Política, se entiende por Sistemas de Información el conjunto de tecnologías o medios tecnológicos, propios o de terceros que gestionen, almacenen o transmitan Información.

2. OBJETIVOS

La presente Política constituye el marco de referencia mediante el que GRUPO SISENER define las directrices de protección eficaz de la Información gestionada por él y tiene los siguientes objetivos:

• Garantizar el grado de confidencialidad necesario a cada clase de Información.

• Mantener la integridad de la información, de modo que no sufra alteraciones con respecto al momento en que haya sido generada por los propietarios o responsables de la misma.

• Asegurar la disponibilidad de la Información, en todos los soportes y siempre que sea necesaria, asegurando la continuidad del negocio y el cumplimiento de cuantas obligaciones sean exigibles a la Compañía.

3. ALCANCE

La presente Política será de aplicación a todas las empresas de GRUPO SISENER.

Asimismo, esta Política podrá ser complementada y desarrollada por las diferentes normas, procedimientos y estándares de Seguridad que se vayan emitiendo para su implantación, las cuales deberán ser coherentes con los principios establecidos en la misma. Las normas de desarrollo adquirirán el mismo carácter vinculante y de obligado cumplimiento.

Cualquier vulneración de la presente Política o de las normas y procedimientos que la desarrollen podrá ser motivo de sanción y, en su caso, dar lugar a las acciones disciplinarias y/o judiciales que se estimen necesarias.

4. PRINCIPIOS GENERALES

La consecución de los objetivos descritos se articula a través de los siguientes principios generales:

- **Clasificación de la Información**. La Información se clasificará en función a su valor, importancia y criticidad para el negocio, de forma que las medidas de protección se adecúen al nivel de clasificación de cada activo de información. Del mismo modo, la clasificación de los activos de Información se realizará tomando en consideración los requisitos legales, operacionales y las buenas prácticas y estándares al respecto.

- **Uso de los Sistemas de Información**. El uso de los Sistemas estará limitado a fines lícitos y exclusivamente profesionales, para la realización de tareas relacionadas con el puesto de trabajo. En consecuencia, estos medios y sistemas no están destinados para uso personal ni podrán utilizarse para ninguna finalidad ilícita.

- **Segregación de funciones**. Se deberán evitar las concentraciones de riesgos derivados de la ausencia de segregación de funciones y la dependencia unipersonal de funciones críticas para el negocio.

En este sentido, se deberán establecer procedimientos formales para controlar la asignación de privilegios a los Sistemas de Información, de forma que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.

- **Retención de la Información**. Se establecerán, cuando resulte necesario o conveniente, períodos de retención de la Información por categorías atendiendo a las necesidades operativas o de cumplimiento regulatorio, así como los correspondientes procedimientos de destrucción de la Información.

- **Acceso a la Información por parte de terceros**. Se desarrollarán los procedimientos de control de la puesta a disposición y acceso por terceros a la Información relativa a GRUPO SISENER o de cualesquiera otros terceros relacionados con el Grupo.

- **Seguridad de la Información en los Sistemas**. Los entornos de desarrollo y producción se mantendrán en Sistemas independientes. Igualmente, el desarrollo y mantenimiento de los Sistemas de Información deben incluir los controles y registros necesarios para garantizar la correcta implementación de las especificaciones de seguridad.

- **Continuidad.** Se establecerá un proceso de gestión de continuidad que permita garantizar la recuperación de la Información crítica para el Grupo en caso de desastre, reduciendo el tiempo de indisponibilidad a niveles aceptables.

- **Cumplimiento**. Los Sistemas de Información y comunicaciones del Grupo deberán estar adecuados de forma permanente a las exigencias de la legislación vigente en todas las jurisdicciones en las que opera, así como a la normativa interna de desarrollo que resulte de aplicación.

5. RESPONSABILIDADES

La responsabilidad de la protección de la Información y de los Sistemas que la tratan, almacenan o transmiten se extiende a todos los niveles organizativos y funcionales de **GRUPO SISENER**, cada uno en la medida que le corresponda, como se detalla a continuación:

1. Responsabilidades de los empleados:

   - Todos los empleados del Grupo deberán conocer, asumir y cumplir la Política, así como la normativa interna de seguridad y uso de los Sistemas vigentes, estando obligados a mantener el secreto profesional y la confidencialidad de la Información manejada en su entorno laboral y debiendo comunicar, con carácter de urgencia y según los procedimientos establecidos, las posibles incidencias o problemas de seguridad que se detecten.

   - Los empleados que contraten servicios de terceros que impliquen el uso o acceso de estos últimos a la Información deberán entender los riesgos derivados del proceso de externalización y asegurar una gestión eficaz de los mismos.

   - El uso de los Sistemas o servicios digitales por parte de los empleados, incluyendo expresamente el correo electrónico y los servicios de mensajería instantánea, estará limitado a fines lícitos y exclusivamente profesionales, para la realización de tareas relacionadas con el puesto de trabajo. En consecuencia, estos medios y sistemas no están destinados para uso personal ni podrán utilizarse para ninguna finalidad ilícita.

2. Responsabilidades en relación con proveedores y otros terceros:

   - Los contratos con terceros que impliquen el uso o acceso de estos últimos a la Información incluirán requerimientos específicos de seguridad relativos a la tecnología y las actividades de aquellos que llevan a cabo dichos servicios.

   - Deberán incluir provisiones mediante las que se garantice que los proveedores, el personal subcontratado o cualquier empresa externa que utilice o acceda, de manera potencial o real, a la Información deberán conocer y cumplir la Política en lo que les sea de aplicación, estando obligados a mantener el secreto profesional y la confidencialidad de la Información manejada en su relación con el Grupo.

3. Responsabilidades del departamento de Sistemas:

El departamento de Sistemas de **GRUPO SISENER** ejercitará su función de control de manera independiente y es responsable de:

- Implementar una estrategia de seguridad de la Información que vele por el cumplimiento de los principios básicos de esta Política, y en particular que dé cobertura a los siguientes aspectos:

  ✓ un adecuado acceso a la Información, basado en el principio de mínimo privilegio y la aprobación del dueño del activo de Información;

- ✓ una segregación adecuada de roles y funciones en los Sistemas de Información;
- ✓ una correcta configuración, administración y operación de la infraestructura, servicios y/o del software utilizado en los distintos procesos de negocio tanto dentro, como fuera de las instalaciones del Grupo, desde el punto de vista de la seguridad;
- ✓ una correcta implementación de los requisitos de seguridad durante el ciclo de vida de los Sistemas de Información que dan soporte a los procesos.
- ✓ una adecuada protección de los Sistemas y la Información que soportan frente a amenazas físicas o ambientales, en atención a su criticidad, que permita identificar, evaluar, prevenir y responder a cualquier riesgo que pueda comprometer su seguridad.

- Establecer y revisar los controles correspondientes para asegurar el cumplimiento de esta Política y su normativa de desarrollo, incluyendo los mecanismos organizativos y tecnológicos necesarios para facilitar la monitorización continua de las actividades del acceso y uso de los Sistemas, servicios o Información gestionados por el Grupo.
- Prevenir, detectar y responder ante cualquier incidente en materia de Seguridad de la Información y actuar de acuerdo con lo Plan de Respuesta ante Incidentes que se apruebe.
- Realizar actividades de formación y concienciación en materia de los procesos de Seguridad de la Información.
- Establecer un enfoque de mejora continua.
- Velar por el cumplimiento con la legislación vigente en el ámbito de las competencias que le atribuye la presente Política.

6. DIFUSIÓN

El órgano de Compliance difundirá la presente Política, a través de los medios que considere apropiados, a todas las partes interesadas en materia de Seguridad de la Información, tanto internas como externas.

7. APROBACIÓN Y VIGENCIA

La Política de Seguridad de la Información ha sido aprobada el 1 de septiembre de 2022 por la Dirección de GRUPO SISENER y estará vigente de forma indefinida, será comunicada a todo el personal y filiales y será objeto de las oportunas acciones de formación y sensibilización.