POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ELABORACIÓN	Fecha: 24/09/2024
	Responsable del Comité de Seguridad
APROBACIÓN	Fecha: 24/09/2024
	72067511R NATALIA ALCITURRI (R: B39024732) Firmado digitalmente por 72067511R NATALIA ALCITURRI (R: B39024732) Fecha: 2024.09.27 10:36:27 +02'00'
	Comité de Seguridad (Representa Rble. Comité de Seguridad)

ÍNDICE **Pág.**

Parque Científico y Tecnológico de Cantabria - C/ Isabel Torres, 7 - 39011 Santander – Cantabria
Tfno. 942 314 224 - Email: semicrol@semicrol.es

1. OBJETO

La Dirección de SEMICROL considera la seguridad de los sistemas de información así como la protección de datos personales factores esenciales para asegurar la prestación de un servicio íntegro, seguro y de calidad a nuestros Clientes y al resto de partes interesadas. Por ello, define esta Política de Seguridad y Privacidad de la Información y asume la máxima responsabilidad en el diseño, implantación y cumplimiento del Sistema de Gestión de Seguridad de la Información y Privacidad.

La Dirección de SEMICROL enfoca la Seguridad de la Información y su Privacidad teniendo en cuenta los requisitos de la actividad de la organización, así como los requisitos legales, reglamentarios o contractuales. Todos los procesos internos y externos quedan adscritos y afectos a la presente política o cuantas políticas transversales se desarrollen para dar cumplimiento a la misma.

La Dirección de SEMICROL ha aprobado esta Política de Seguridad y Privacidad de la Información y permanecerá vigente mientras no se apruebe una modificación de la misma. La Política es comunicada y puesta a disposición de todos los afectados, tanto internos como externos.

2. ALCANCE

El Sistema de Gestión de la Seguridad de la Información y Privacidad (en adelante SGSIP) se ha desarrollado tomando como alcance, según las normas ISO/IEC 27001 e ISO/IEC 27701 y en el Esquema Nacional de Seguridad:

Los sistemas de información que dan soporte a los servicios de:

- Consultoría tecnológica y de procesos
- Proceso de integración, desarrollo y mantenimiento de sistemas y aplicaciones informáticas e implantación y mantenimiento de Fundanet como SaaS y On-premise.

3. MISIÓN

La misión de SEMICROL se encuentra recogida en el apartado *Misión, Visión y Valores* de la intranet de la organización.

4. COMPROMISOS DE LA DIRECCIÓN

La Dirección de SEMICROL está comprometida con el desarrollo e implementación del Sistema de Gestión de Seguridad de la Información y Privacidad y con la mejora continua de su eficacia.

La Gerencia ostenta el cargo de Responsable del Comité de Seguridad y como tal desempeña las siguientes funciones:

- Comunica a la organización la importancia de satisfacer tanto los requisitos del cliente como los de seguridad, del servicio, los legales, reglamentarios, y las obligaciones contractuales.
- Establece y comunica el alcance del SGSIP.
- Define y comunica la Política de Seguridad y Privacidad, normas y procedimientos.

Parque Científico y Tecnológico de Cantabria - C/ Isabel Torres, 7 - 39011 Santander – Cantabria
Tfno. 942 314 224 - Email: semicrol@semicrol.es

- Comunica la Política de Seguridad y Privacidad y la importancia de cumplir con ella a clientes y a proveedores (contrato de confidencialidad).
- Asegura el establecimiento y la comunicación de los objetivos de seguridad de la Información.
- Lleva a cabo las revisiones por la Dirección anuales.
- Dirige las revisiones del SGSIP.
- Vela por que se realicen las auditorías internas del SGSIP, anualmente.
- Asegura que se revisan los resultados de las auditorías para identificar oportunidades de mejora.
- Asegura la provisión y disponibilidad de recursos.
- Asegura que se gestionan y se evalúan los riesgos de seguridad de la información y privacidad, a intervalos planificados.
- Define el enfoque a tomar para la gestión de los riesgos de seguridad de la información y privacidad y los criterios para asumir los riesgos.
- Aprueba los niveles de riesgo aceptables para la organización.
- Establece roles y responsabilidades en materia de seguridad.
- Determina las cuestiones externas e internas que son pertinentes para el propósito de la organización y su dirección estratégica.

El compromiso de la Dirección está reflejado en la siguiente política.

5. POLÍTICA DE SEGURIDAD Y PRIVACIDAD

La **Política de Seguridad y Privacidad** tiene por objeto asegurar la continuidad del negocio, proteger tanto los activos de información de la organización como los activos de información y datos personales de nuestros clientes y partes interesadas, con los que exista un acuerdo contractual. Esto incluye minimizar los posibles riesgos de ataque o vulneración, ante cualquier amenaza, sea interna o externa, deliberada o accidental, y garantizar el cumplimiento de las normativas de privacidad. Se busca contribuir a la prestación de un servicio íntegro, seguro, de calidad y que respete la privacidad de nuestros Clientes y del resto de partes interesadas, garantizando tanto la calidad como la confidencialidad de la información y los datos personales. SEMICROL actúa de forma preventiva, supervisa la actividad diaria para detectar cualquier incidente de seguridad o privacidad y reacciona con urgencia a los incidentes, buscando recuperarse lo antes posible y minimizar el impacto sobre la seguridad de la información y la protección de los datos personales.

SEMICROL tiene implantado, y mejora continuamente, un Sistema de Gestión de Seguridad de la Información y Privacidad acorde con la ISO/IEC 27001, la ISO/IEC 27701 y el Esquema Nacional de Seguridad.

La Política de Seguridad y Privacidad es de aplicación para todo el personal de la organización, incluyendo sus proveedores y el personal contratado temporalmente; afecta a cualquier tipo de información y datos personales, tanto la que sea propiedad de la organización como la que procede de clientes o partes interesadas, con independencia del soporte o medio en el que se encuentre, tipología o categoría; y aplica a cualquier activo de información y datos personales propiedad de la organización o gestionado en nombre de terceros que afecte al sistema.

Parque Científico y Tecnológico de Cantabria - C/ Isabel Torres, 7 - 39011 Santander – Cantabria
Tfno. 942 314 224 - Email: semicrol@semicrol.es

Toda violación de la presente política o aquellas que la desarrollen, de las normas y procedimientos, será considerado por el procedimiento disciplinario, incluyéndose proveedores y colaboradores externos que serán tramitados por su procedimiento oportuno.

5.1 Objetivos

- Mantener una gestión adecuada del SGSIP de acuerdo con los estándares de seguridad y privacidad y las buenas prácticas del sector, llevando a cabo todo esto de manera que se aseguren ventajas competitivas para la organización.
- Cumplir con los requisitos de negocio, las obligaciones legales y las obligaciones contractuales de seguridad y privacidad, así como con las normativas aplicables sobre protección de datos.
- Proteger la información, los datos personales y los sistemas que la sustentan desde el punto de vista de las siguientes dimensiones de seguridad:
    - Confidencialidad: característica consistente en que la información y los datos personales ni se ponen a disposición, ni se revelan a individuos, entidades o procesos no autorizados.
    - Integridad: característica consistente en que el activo de información y los datos personales no han sido alterados de manera no autorizada.
    - Disponibilidad: característica de los activos y los datos personales consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
    - Trazabilidad: característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
    - Autenticidad: característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden sus datos.
- Desarrollar un proceso de análisis del riesgo y, de acuerdo a su resultado, implementar las acciones, controles y procedimientos necesarios con el fin de tratar los riesgos que se consideren no asumibles por SEMICROL.
- Reflejar en la Declaración de Aplicabilidad del SGSIP las medidas de seguridad, controles y dimensiones definidos en el Esquema Nacional de Seguridad, en la ISO/IEC 27001 y en ISO/IEC 27701.
- Realizar, al menos una vez al año, una revisión global del Sistema para valorar su eficacia y analizar el estado de los objetivos fijados en relación a la Seguridad de la Información, con el fin de establecer los nuevos para el siguiente ciclo, que garanticen la mejora continua del SGSIP, siendo consistentes con los presentes objetivos.
- Establecer y difundir los roles y responsabilidades relacionados con la Seguridad de la Información y la Protección de Datos Personales.
- Concienciar y formar con regularidad a todo el personal de la organización en cuanto a la seguridad de la información y privacidad.
- Establecer los medios necesarios para garantizar la continuidad del negocio de la organización.

Parque Científico y Tecnológico de Cantabria - C/ Isabel Torres, 7 - 39011 Santander – Cantabria
Tfno. 942 314 224 - Email: semicrol@semicrol.es

- Asegurar que se establecen la normativa y procedimientos pertinentes para cumplir con esta Política y, en particular, asegurar que las incidencias de seguridad son comunicadas y tratadas apropiadamente.
- Sancionar cualquier violación a esta política, así como a cualquier norma o procedimiento del SGSIP.

5.2 Legislación aplicable y requisitos contractuales

En el documento *Legislación y Normativa* se identifican las obligaciones legales aplicables a la organización en relación a la seguridad de la información y la protección de datos personales.

Además, se consideran los requisitos contractuales establecidos en contratos de clientes o proveedores que requieren de requisitos específicos en materia de seguridad y privacidad.

5.3 Organización de Seguridad

La organización de la seguridad en SEMICROL se estructura a través del Comité de Seguridad. Este Comité está constituido por: el Responsable de la Información, el Responsable del Servicio, el Responsable del Comité de Seguridad, el Responsable del SGI, el Responsable de Seguridad, el Responsable del Sistema y el Delegado de Protección de Datos.

Se designa al Responsable de Seguridad como el POC (Persona de Contacto) de la organización en materia de seguridad.

Las funciones y responsabilidades, tanto del Comité de Seguridad, como de cada uno de los roles de seguridad que constituyen el mismo, así como el procedimiento de resolución de conflictos de responsabilidades, se encuentran definidos en el *Manual del Sistema de Gestión – Sección 03*. El procedimiento para su designación y renovación se encuentra definido en el *proceso E02. Seguridad de los Sistemas de Información – Anexo 3.*

Los roles y responsabilidades en relación al SGSIP son comunicados a las nuevas incorporaciones y recordados periódicamente a todo el personal de la organización.

5.4 Documentación de seguridad del sistema

La documentación generada dentro del SGSIP es controlada y aprobada por el Comité de Seguridad.

Esta documentación se encuentra localizada en un proyecto de la aplicación de gestión, de acceso restringido para los miembros del Comité de Seguridad, únicamente haciéndose públicos los documentos que se considere que deben ser conocidos por todos a través de su publicación en la Intranet o de la asignación de permisos específicos.

En el procedimiento *A04. Control de la Documentación* se establece la gestión que se realiza de la documentación del SGSIP, y en el *Anexo 7* del procedimiento *E02. Seguridad de los Sistemas Información*, se especifica la calificación de la información.

Parque Científico y Tecnológico de Cantabria - C/ Isabel Torres, 7 - 39011 Santander – Cantabria
Tfno. 942 314 224 - Email: semicrol@semicrol.es

5.5 Principios básicos y requisitos mínimos de seguridad

Esta Política de Seguridad, se establece de acuerdo con los principios básicos de seguridad establecidos en el artículo 5 del RD 311/2022:

a) Seguridad como proceso integral
b) Gestión de la seguridad basada en los riesgos
c) Prevención, detección, respuesta y conservación
d) Existencia de líneas de defensa
e) Vigilancia continua
f) Reevaluación periódica
g) Diferenciación de responsabilidades

Y se desarrolla aplicando los siguientes requisitos mínimos, establecidos en el artículo 12 del RD 311/2022:

a) Organización e implantación del proceso de seguridad
b) Análisis y gestión de los riesgos
c) Gestión de personal
d) Profesionalidad
e) Autorización y control de los accesos
f) Protección de las instalaciones
g) Adquisición de productos de seguridad y contratación de servicios de seguridad
h) Mínimo privilegio
i) Integridad y actualización del sistema
j) Protección de la información almacenada y en tránsito
k) Prevención ante otros sistemas de información interconectados
l) Registro de la actividad y detección de código dañino
m) Incidentes de seguridad
n) Continuidad de la actividad
o) Mejora continua del proceso de seguridad

Parque Científico y Tecnológico de Cantabria - C/ Isabel Torres, 7 - 39011 Santander – Cantabria
Tfno. 942 314 224 - Email: semicrol@semicrol.es