POLÍTICA

PO.SG

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Innovasur
Julio 2022

Confidencialidad Acerca de este documento

Innovasur

Parque Científico y Tecnológico Geolit, C/Sierra Morena,12-A
23630, Mengíbar, Jaén
ESPAÑA
www.innovasur.com

1. INTRODUCCIÓN, OBJETO Y ALCANCE

1.1. INTRODUCCIÓN

La información relativa al negocio de **Innovaciones Tecnológicas del Sur, S.L.**, en adelante **Innovasur,** requiere de protección contra el uso indebido, la revelación, el robo, la alteración o destrucción de la misma. La gestión efectiva de la seguridad de la información permite compartir dicha información minimizando la exposición a riesgos.

Esta política es la piedra angular del programa global de seguridad de la información, dirigido a la protección de los activos de información incluidos dentro del alcance del Sistema de Gestión de Seguridad de la Información (en adelante, SGSI). Esta política está basada en la Normativa General de Seguridad de la Información.

Esto implica que se deben aplicar las medidas de seguridad de la información dispuestas en las siguientes normas:

- **ISO/IEC 27001:2013:** Sistema de Gestión de la Seguridad de la Información (SGSI).
- **Esquema Nacional de Seguridad (ENS):** Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, aplicable a empresas privadas que desarrollan funciones, misiones, cometidos o servicios para las Administraciones Públicas.

Esta Política de Seguridad asegura un compromiso manifiesto de la dirección de la organización para la difusión, consolidación y cumplimiento de la presente Política.

1.2. OBJETO

El objeto de esta política es establecer un marco de trabajo que permita identificar, desarrollar e implantar las medidas técnicas y organizativas necesarias para garantizar la seguridad y protección tanto de la información relativa a servicios como de los sistemas que la gestionan, y definir la política de continuidad de **Innovasur.**

1.3. ALCANCE

El alcance del SGSI corresponde a los ***Sistemas de Información que dan soporte a la prestación de Servicios de consultoría, instalación, soporte y mantenimiento de sistemas de información, telecomunicaciones y Centro de Operaciones de Seguridad de Innovaciones Tecnológicas del Sur S.L. para empresas y Administraciones Públicas*****,** de acuerdo con el documento de aplicabilidad vigente.

Con esta política de **seguridad de la información**, la organización muestra su compromiso por establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de acuerdo a los requisitos definidos en la norma ISO/IEC 27001:2013 y los principios recogidos en el artículo 4 del real decreto 3/2010. Esto es:

- Entender la seguridad como un proceso integral.

- Gestionar la seguridad basándonos en los riesgos.
- En una contínua monitorización y vigilancia de los eventos de seguridad para su pronta detección y respuesta.
- Establecer defensas
- Evaluar el estado de la seguridad periódicamente

2. MISIÓN Y OBJETIVOS

La organización, en el empeño por cumplir los intereses, funciones y competencias propias de la actividad que desempeña , pone a disposición de la sociedad y de sus partes interesadas los servicios y actividades necesarios para satisfacer las aspiraciones y expectativas de sus clientes y usuarios. Para ello, **Innovasur** hace uso de las tecnologías apropiadas con objeto de crear la confianza necesaria entre sus clientes y usuarios basada en un sistema de seguridad de la información integral.

Estos sistemas pretenden garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes. Para ello, se establecen como objetivos generales en materia de seguridad de la información los siguientes:

1. Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos personales y a la prestación de servicios a través de medios electrónicos.
2. Asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con rapidez a los incidentes.
3. Proteger los recursos de información de la organización y la tecnología utilizada para su procesamiento frente a amenazas, internas o externas, deliberadas o accidentales.
4. Proporcionar confianza a las partes interesadas de la organización protegiendo su información durante todo su ciclo de vida.
5. Facilitar la mejora continua de los procesos de seguridad, procedimientos, productos y servicios.
6. Cumplir los requisitos legales de negocio y otros requisitos de clientes (explícitos e implícitos) relacionados con seguridad de la información.
7. Garantizar la continuidad de la organización estableciendo proyectos de contingencia en los servicios críticos y manteniendo en todo momento la seguridad.
8. Garantizar que se provean los recursos necesarios para garantizar la seguridad, así como asignar funciones y responsabilidades al personal encargado de mantener el SGSI.
9. Concienciar, formar y motivar al personal de **Innovasur** sobre la importancia del desarrollo e implantación del SGSI para los objetivos estratégicos de negocio y su implicación para su correcta consecución.

3. MARCO NORMATIVO

Para el desarrollo de las actividades comprendidas en el alcance de esta política de seguridad, se establece un marco normativo y legislativo sobre los que se sustenta la prestación de los servicios:

De ámbito Europeo:

- Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas del mercado interior (Idas) y normas de ejecución.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE.
- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016. (NIS)

De ámbito Estatal:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Resolución de 7 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas, por el que se aprueba la Instrucción Técnica de Seguridad de Informe de Estado de Seguridad.
- Resolución de 13 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas, por el que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Ley 2/2019, de 1 de marzo, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del

Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

De ámbito Autonómico:

- Ley 1/2014 de 24 de junio de Andaluza de Transparencia Pública de Andalucía

De ámbito Normativo:

- ISO/IEC 27001:2013

4. ORGANIZACIÓN DE LA SEGURIDAD

Para gestionar y coordinar proactivamente la seguridad de la información en **Innovasur,** se constituye el **COMITÉ DE SEGURIDAD DE LA INFORMACIÓN** como órgano de gestión.

Este **Comité de Seguridad** será el órgano encargado de aprobar esta política de seguridad y será el responsable de la autorización de sus modificaciones, así como de toda la información documentada del SGSI/ENS de la entidad.

Este Comité estará constituido, al menos, por los siguientes cargos:

- Responsable de Seguridad de la Información
- Responsable del Servicio
- Responsable de Seguridad
- Responsable del Sistema
- Administrador de la seguridad
- Delegado de Protección de Datos
- Secretario/a del Comité
- Responsable del Sistema de Gestión

Las funciones y responsabilidades a desempeñar por los mismos, serán las siguientes:

a. RESPONSABLE DE LA INFORMACIÓN
Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. Asesorará y tendrá potestad para determinar técnicamente los requisitos de la información y de los servicios en materia de seguridad. Tendrá la potestad, igualmente, de determinar los niveles de seguridad de la información.

Así mismo informará sobre el estado de la seguridad en el área de los sistemas de la información y comunicación. Podrá convocar las reuniones, remitir información y comunicados a los miembros de la comisión.

b. RESPONSABLE DE SERVICIO

Será la persona o personas responsables de la explotación de las distintas áreas de la entidad estableciendo requisitos, fines y medios para la realización de dichas tareas. Determinará los requisitos de seguridad de los servicios prestados. Esto incluye la responsabilidad de determinar los niveles de seguridad de los servicios y para ello, podrá recabar asesoramiento del responsable de seguridad y del responsable del sistema.
Incluirá las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control. Tendrá, además, la misión de valorar las consecuencias de un impacto negativo sobre la seguridad de los servicios, teniendo en consideración la repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de las personas.

Además, tendrán la obligación de vigilar el cumplimiento de las normas de seguridad dentro de su área e informar al Responsable de la Información del cumplimiento de la normativa de seguridad aprobada por el Comité de Seguridad.

c. RESPONSABLE DE LA SEGURIDAD
Es la persona designada por el máximo órgano de gobierno para la supervisión del sistema de seguridad de la información y será el encargado de determinar las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.
Las dos funciones esenciales del Responsable de la Seguridad son:

a. Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en esta Política de Seguridad de la Información de la organización.
b. Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Si el sistema de información, dado su complejidad, distribución, separación física o número de usuarios así lo requiriera, la organización podrá designar Responsables de Seguridad Delegados, en los que se podrá delegar funciones, pero nunca responsabilidades. Estos Responsables de Seguridad Delegados tendrán dependencia directa del Responsable de Seguridad.

Entre las funciones que se le atribuyen al Responsable de Seguridad, se encuentran las siguientes:

- Coordinará y controlará las medidas definidas en el Registro de Actividades del Tratamiento y en general se encargará del cumplimiento de las medidas de seguridad que detalla el informe de evaluación de impacto en la protección de datos.
- Reportará directamente al Comité de Seguridad de la Información.
- Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y realizará la categorización del Sistema.
- Realizará el Análisis de Riesgos.
- Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.

- Facilitará a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
- Coordinará la elaboración de la Documentación de Seguridad del Sistema.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política de Seguridad de la Información, para su aprobación.
- Participará en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de la normativa de Seguridad de la Información.
- Elaborará los Procedimientos Operativos de Seguridad de la Información.
- Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).
- Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
- Analizará y propondrá salvaguardas que prevengan incidentes similares en caso de que estos se hubieran producido.
- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información.
- Elaborará los Planes de Continuidad de Sistemas que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas.
- Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

d. RESPONSABLE DEL SISTEMA

Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad. Su responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados. Sus funciones, de manera concreta, son las siguientes:

a. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
b. Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
c. Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
d. El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.

e. Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.
f. Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
g. Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.
h. Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.

Si el sistema de información, dado su complejidad, distribución, separación física o número de usuarios requiriera personal adicional para el desempeño de estas funciones, la organización podrá designar Responsables del Sistema Delegados, en los que se podrá delegar funciones, pero nunca responsabilidades. Estos Responsables del Sistema Delegados tendrán dependencia directa del Responsable de Seguridad.

e. ADMINISTRADOR DE LA SEGURIDAD
Sus funciones más significativas serían las siguientes:

a. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

b. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.

c. La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.

d. La aplicación de los Procedimientos Operativos de Seguridad (POS).

e. Asegurar que los controles de seguridad establecidos son adecuadamente observados.

f. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.

g. Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

h. Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

i. Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

j. Colaborar en la investigación y resolución de incidentes de seguridad, desde su

detección hasta su resolución.

En emplazamientos donde se encuentren ubicados varios sistemas de información, la función de AS podría recaer en la misma persona, para todos ellos.

f. DELEGADO DE PROTECCIÓN DE DATOS.

Velará y asesorará para proteger el cumplimiento de los derechos de los interesados en materia de protección de datos. Además, supervisará y asesorará en la evaluación de impacto de los tratamientos de datos de caracter personal y evaluación de los riesgos de estos tratamientos de datos.

g. SECRETARIO/A

Las funciones de Secretaría del Comité de Seguridad serán asumidas por el Responsable del Sistema de Gestión, y tendrán como funciones la preparación de las reuniones, la difusión de sus resultados y el seguimiento de los acuerdos alcanzados.

PROCEDIMIENTOS DE DESIGNACIÓN

Cada uno de los responsables que formarán parte del comité de seguridad serán nombrados por la dirección de la entidad. Los nombramientos se revisarán cada 2 años o cuando el puesto quede vacante o cambie.

FUNCIONES DEL COMITÉ DE SEGURIDAD

El Comité de Seguridad reportará a la Dirección. El Comité de Seguridad, en lo que se refiere al SGSI y al cumplimiento de lo dispuesto en el ENS, tendrá las siguientes funciones:

- Responsabilidades derivadas del tratamiento de datos personales.
- Atender las inquietudes de la organización y de las diferentes áreas.
- Informar regularmente del estado de la seguridad de la información a dirección.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a la seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para que sea aprobada por el propio Comité de Seguridad antes de su aprobación final.
- Aprobar la normativa de seguridad de la información.
- Evaluar los riesgos de manera periódica para establecer las adecuadas medidas de seguridad necesarias atendiendo a los resultados.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.

- Monitorizar los principales riesgos residuales asumidos por **Innovasur** y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Establecer medidas adecuadas para la formación, información y concienciación de todo el personal en materia de seguridad de la información y protección de datos de carácter personal.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

El Comité de Seguridad de la Información no es un comité técnico, pero recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones. El Comité de Seguridad de la Información se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Grupos de trabajo especializados internos, externos o mixtos.
- Asesoría externa.
- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

5. REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad de la Información la revisión anual de esta Política de Seguridad de la Información y la propuesta de modificación o mantenimiento de la misma. La Política será aprobada por el Rector y difundida para que la conozcan todas las partes afectadas.

6. GESTIÓN DE LA DOCUMENTACIÓN

Se deberá comunicar la información documentada relativa a los controles de seguridad al personal que trabaja en la entidad (empleados y proveedores), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de ese modo, al cumplimiento de los requisitos del ENS.

La información documentada será clasificada conforme a los descrito en la normativa de clasificación de la información, estableciéndose el uso adecuado de la misma de acuerdo a dicha clasificación.

7. COMUNICACIÓN DE LA POLÍTICA DE SEGURIDAD

Esta Política determina las bases de políticas, normativas y procedimientos de seguridad que afrontan aspectos específicos. La Política de seguridad estará a disposición de todas las partes interesadas definidas por la organización conforme a la política de comunicación establecida, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones dentro del alcance SGSI.

Las políticas, normativas y procedimientos de seguridad estarán disponibles de manera interna para todo el personal de **Innovasur**.

8. PERSONAL, FORMACIÓN Y CONCIENCIACIÓN

Con carácter anual se realizarán las acciones de formación y concienciación en materia de seguridad necesarias alcanzar los siguientes objetivos:

- Mantener informado al personal más directamente relacionado con el manejo de información y los sistemas que la tratan sobre los procedimientos existentes de seguridad, riesgos, medidas de protección, planes de protección, etc.
- Concienciar al personal, en general, de la importancia de la seguridad y de los procedimientos básicos de manejo e intercambio de información.

Las áreas responsables determinarán el formato de la acción de Formación y Concienciación, así como sus contenidos. Dentro de Innovasur siempre se buscará tener personal con la adecuada cualificación para prestar sus servicios con la adecuada madurez y gestión.

También será responsabilidad del responsable del servicio velar y hacer cumplir el principio de mínimo privilegio y seguir el procedimiento de autorización con objeto de velar por que dentro de su servicio la información accesible sea estrictamente confidencial y la indispensable para el desempeño de las tareas derivadas de su puesto.

9. GESTIÓN DE RIESGOS

Innovasur realizará periódicamente y cada vez que los sistemas de la información sufran una alteración significativa un Análisis de Riesgos, de modo que se puedan anticipar los riesgos

existentes. Este Análisis de Riesgos y sus conclusiones han de ser analizadas por el Comité de Seguridad y establecer las salvaguardas adecuadas para que el nivel de riesgo sea aceptable.

10. GESTIÓN DE INCIDENTES Y REGISTROS DE ACTIVIDAD

Innovasur se compromete a disponer los procedimientos para la gestión de incidentes de seguridad y continuidad de negocio necesarios para minimizar el impacto de los mismos.

También se compromete a comunicar a las partes interesadas los incidentes y guardar registros de la actividad con objeto de estudiar el incidente y prevenir que vuelva a suceder en esta organización.

11. CONTINUIDAD DE SERVICIO

Innovasur se compromete a disponer los procedimientos para la evaluación de impacto y disponer las medidas técnicas y organizativas necesarias para conseguir mantener sus servicios activos y garantizar la pronta recuperación de los mismos. Para ello realizará evaluaciones de recuperación del sistema y se evaluarán anualmente para establecer puntos de mejora.

12. DATOS PERSONALES

Innovasur únicamente recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos, y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativa necesarias para el cumplimiento de la normativa de Protección de Datos. Estas medidas estarán recogidas en las políticas, normativas y procedimientos que emanan de la presente política de seguridad.

13. COMPROMISO DE LA DIRECCIÓN

La Dirección de **Innovasur** manifiesta su compromiso formal con el apoyo a los planes de seguridad que se deriven de la aplicación de esta Política. Dicho apoyo se concretará en:

- proporcionar los recursos necesarios, dentro de las posibilidades presupuestarias;
- asignar roles y responsabilidades a las personas asociadas a los planes de seguridad;
- destinar presupuesto, dentro de las posibilidades;
- apoyar la formación de los recursos humanos implicados en los planes de seguridad para que adquieran el nivel de concienciación y las competencias necesarias;
- garantizar el mantenimiento de la documentación asociada a los planes de seguridad;
- facilitar las comunicaciones con otras organizaciones en materia de seguridad de la información;

- promover la mejora continua.

El compromiso con el apoyo a los planes se manifiesta con la aprobación del presente documento.

14. APROBACIÓN Y ENTRADA EN VIGOR

La presente Política de Seguridad de la Información será aprobada por el Comité de Seguridad mediante firma y será difundida a las partes interesadas de Innovasur.

Así mismo, el Comité dotará de los recursos necesarios para la aplicación efectiva de esta política, y para su buen desarrollo, tanto en las actividades de implantación como en su posterior mantenimiento y mejora de todo el SGSI de la entidad.