SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Innovaciones Tecnológicas del Sur, S.L.

GEOLIT

Parque Científico y Tecnológico

C/ Sierra Morena Nº12, A

23620 Mengíbar, Jaén

ESPAÑA

https://www.innovasur.com/

TABLA DE CONTENIDOS

1. INTRODUCCIÓN, OBJETIVO Y ALCANCE 3
1.1. INTRODUCCIÓN 3
1.2. OBJETIVO 3
1.3. ALCANCE 3
2. POLÍTICA DE SEGURIDAD 4
3. OBJETIVOS 4
4. RESPONSABILIDADES 4
5. REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN 6
5.1. PROCESO DE REVISIÓN DE LA POLÍTICA 7
6. VIOLACIÓN DE LA POLÍTICA DE SEGURIDAD 9
7. COMUNICACIÓN DE LA POLÍTICA DE SEGURIDAD 9
8. FORMACIÓN Y CONCIENCIACIÓN 9
9. GESTIÓN DE RIESGOS 9
10. DATOS PERSONALES 10
11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD 10
12. COMPROMISO DE LA DIRECCIÓN 10
13. APROBACIÓN Y ENTRADA EN VIGOR 11

1. INTRODUCCIÓN, OBJETIVO 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 dispuestas en las siguientes normas:

- **ISO/IEC 27001:2015:** 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.

1.2. OBJETIVO

El objetivo 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 los Servicios de consultoría, instalación, soporte y mantenimiento de sistemas de información y telecomunicaciones de Innovaciones Tecnológicas del Sur S.L. para empresas y Administraciones Públicas** de acuerdo con el documento de aplicabilidad.

Las áreas detalladas a continuación relacionan los objetivos y controles definidos en la ISO 27001 y en el ENS, ajustándose al negocio de Innovasur, así como a su entorno de seguridad.

- Política de Seguridad de la Información.
- Organización de Seguridad de la Información.
- Gestión de Activos.
- Seguridad relativa a los Recursos Humanos.
- Seguridad Física y del Entorno.
- Control de Acceso.
- Criptografía.
- Seguridad de las Operaciones.

- Seguridad de las Comunicaciones.
- Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.
- Gestión de Incidentes de Seguridad de la Información.
- Relación con proveedores.
- Gestión de Continuidad de Negocio.
- Cumplimiento legal.

Dichos aspectos se relatan en detalle en la Normativa General de Seguridad de la Información.

2. POLÍTICA DE SEGURIDAD

La presente Política de Seguridad de la Información ha sido desarrollada para asegurar la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios, junto con la tecnología y los activos de información de Innovasur (p.e. aplicaciones, redes o los propios servicios) y se alinea con la ISO 27001 y el ENS.

3. OBJETIVOS

El SGSI tiene como objetivo principal asegurar la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios, junto con la tecnología y los activos de información de Innovasur, según el documento de aplicabilidad.

Los objetivos genéricos que Innovasur ha establecido para cumplir a lo largo del tiempo son:

- Proporcionar la confianza a los clientes protegiendo su información durante todo su ciclo de vida.
- Facilitar la mejora continua de los procesos de seguridad, procedimientos, productos y servicios.
- Cumplir los requisitos legales de negocio y otros requisitos de clientes (explícitos e implícitos) relacionados con seguridad de la información.
- Garantizar la Continuidad del Negocio estableciendo proyectos de contingencia en los servicios críticos manteniendo en todo momento la seguridad.
- Garantizar que se provean los recursos necesarios para garantizar la seguridad, así como asignar funciones y responsabilidades al personal encargado de mantener el SGSI.
- 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.

4. RESPONSABILIDADES

El Comité de Seguridad de la Información formado por personal cualificado en materia de seguridad, procederá a revisar y a proponer la aprobación de la presente Política de Seguridad de la Información a la Dirección de Innovasur que será el **Responsable de la Información**:

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

- El **Responsable de Seguridad de la Información**, cuya figura recae en el propio Responsable de los servicios objeto de alcance, será el encargado de notificar la presente política al personal de la entidad y de los cambios que en ella se produzcan, así como de coordinar las acciones de implantación, mantenimiento y mejora del SGSI/ENS de la entidad, y de sus auditorías, con el **Responsable de Sistemas** cuya figura recae en el propio Responsable de Sistemas de Innovasur, que se encargará de gestionar los requisitos técnicos de seguridad de los sistemas de información, y con el **Responsable del Servicio** que se encargará de gestionar los requisitos de seguridad de las actividades de su área para la prestación de los servicios.
- **Todo el personal** de Innovasur, tanto interno como externo, será responsable de cumplir con la presente Política de Seguridad de la Información dentro de su área de trabajo, así como de aplicar toda la información documentada de los controles y medidas de seguridad del SGSI/ENS de Innovasur en sus actividades laborales que afecta a su desempeño en seguridad de la información.

El detalle de las responsabilidades antes indicadas, así como los roles y autoridades en materia de seguridad de la información, se detallan a continuación:

- **Comité de Seguridad.**
  - Revisión y aprobación de la Política Corporativa de Seguridad de la Información y de las responsabilidades principales.
  - Supervisión y control de los cambios significativos en los sistemas de información y en la organización de la compañía que puedan afectar, desde el punto de vista de la seguridad, a los activos de información.
  - Revisión y seguimiento de incidencias de Seguridad de la Información.
  - Aprobación de las iniciativas principales para mejorar la Seguridad de la Información, así como del Plan de Acción.
  - Coordinación de las acciones que requieran intervención de otras áreas de la compañía.
  - Reporte a la Dirección de las principales acciones desarrolladas durante el año, así como de la situación en materia de seguridad de la compañía. Asimismo, informará a la Dirección en las situaciones de crisis o de carácter excepcional.
- **Responsable de la Información.**
  - Establecerá el nivel de seguridad que la información y los servicios prestados por Innovasur requieren en base a sus exigencias en cuanto a disponibilidad, confidencialidad e integridad, considerando el impacto que tendría en los clientes y en la propia Organización la falta de alguno de esos aspectos. Será nombrado por la persona que disponga del máximo cargo dentro de la Organización.
- **Responsable de Seguridad de la Información.**
  - Esta figura recae sobre el propio Responsable de los Servicios.
  - Tiene la facultad de establecer los requisitos en materia de seguridad de la información gestionada. Si esta información incluye datos de carácter personal, además, deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.
  - Determina los niveles de seguridad de la información.
- **Responsable del Sistema.**

- Definir, en coordinación con el Responsable de Seguridad de la Información, las especificaciones funcionales de seguridad de los Sistemas de Información de la Organización.
- Garantizar que en el diseño de sistemas de información y redes de comunicaciones se contemplen desde el principio los aspectos necesarios de seguridad de la información en cuanto a disponibilidad, integridad, confidencialidad, autenticación, control de acceso, auditoría y registro.
- Revisar que la configuración de seguridad tras la instalación de un sistema nuevo es la adecuada.
- Revisar que la configuración de seguridad tras los cambios en un sistema sigue siendo la adecuada.
- Verificar el funcionamiento de mecanismos de Control de Acceso que eviten que un usuario acceda a datos o recursos con derechos distintos de los autorizados, sin que en ningún caso se puedan desactivar.
- Seguir los foros de vulnerabilidades y elaboración del calendario de aplicación de parches para los sistemas de información, en función de los que surjan y el impacto que tengan en la seguridad (los parches mismos los aplicarán los administradores de sistemas).
- Implantar las medidas de seguridad que resulten de los planes de tratamiento de riesgos o planes de acciones correctivas a raíz de las auditorías de seguridad de la información.
- Proporcionar datos para la alimentación de indicadores de seguridad de la información.
- Supervisar los procedimientos de copias de seguridad.
- Realizar auditorías técnicas periódicas de la infraestructura, sistemas y aplicaciones.

- **Responsable del Servicio:**
  - Establece los requisitos del servicio en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios.
  - Realizar propuestas al Responsable de la Seguridad con la opinión del Responsable del Sistema.

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

La revisión de la política de seguridad tiene como objetivo ajustar la política a los cambios que puedan afectar a las directrices de la política inicialmente establecidas para los riesgos identificados. Dichos cambios pueden ser cambios en la organización, identificación de vulnerabilidades importantes o cambios importantes en la infraestructura técnica.

Las reuniones del Comité de Seguridad se realizan con una periodicidad anual, aunque cualquier miembro fijo del Comité puede convocar reuniones extraordinarias cuando lo entienda necesario, bien sea como respuesta a incidentes, como cambios organizativos o cualquier otro aspecto que pueda afectar al SGSI/ENS.

En cualquier caso, los temas que se tratarán de manera sistemática son: Cambios en el entorno, Incidentes de seguridad e Iniciativas de Seguridad.

La salida de las revisiones gerenciales de la Política debe incluir decisiones y acciones relacionadas con mejoras para manejar la seguridad de la información y los procesos, mejoras en objetivos de control y controles o mejoras de asignación de recursos y/o responsabilidades.

Las reuniones podrán tener carácter físico o virtual y dispondrán de actas en las cuales se recogerá evidencia al menos uno de los asuntos tratados y los acuerdos alcanzados. Estas formarán parte de los registros del Sistema y quedarán almacenadas, con carácter confidencial, en la Intranet de Innovasur.

5.1. PROCESO DE REVISIÓN DE LA POLÍTICA

Al menos una vez al año, se realizará una Revisión Global del SGSI en la que se llevarán a cabo las siguientes acciones:

- Revisión de la adecuación de la Política de Seguridad.
- Revisión y aseguramiento del cumplimiento de los objetivos.
- Planteamiento de objetivos para siguientes períodos.
- Comprobación de que se mantiene constante la eficacia y adecuación del SGSI implantado, de modo que se garantice que está funcionando adecuadamente.

El proceso de evaluación se realiza en los siguientes pasos, el resultado de los cuales se incluirá en el acta de revisión por la dirección:

1. **Planificación**

El Responsable de Seguridad organiza y comunica el inicio del proceso de revisión. Planifica la revisión y define las acciones a realizar por cada uno de los participantes en la revisión, además de sus responsabilidades y plazos de ejecución. Durante esta planificación se consideran relevantes para ser tenidas en cuenta en el proceso de revisión:

- Retroalimentaciones de las partes interesadas.
- Resultados de revisiones independientes.
- Estado de acciones preventivas y correctivas anteriores.
- Resultados de revisiones gerenciales previas.
- Cambios en el ambiente organizacional, circunstancias comerciales, disponibilidad de recursos, condiciones contractuales, reguladoras, legales o de ambiente técnico.
- Tendencias de amenazas/vulnerabilidades.
- Incidentes de seguridad reportados.
- Recomendaciones realizadas por autoridades relevantes.

2. **Ejecución de la Revisión**

Se procede a evaluar por parte de los participantes en la revisión, los inputs del proceso de revisión de la Política dentro de su ámbito de actuación. En esta fase se identifican los posibles aspectos que provoquen cambios en la Política y otros a considerar de acuerdo con cambios técnicos, organizativos, legales o de entorno.

3. **Reunión de Revisión de Resultados**

Se organiza una reunión donde se identifican los aspectos a partir de los cuales es preciso modificar la Política de Seguridad definida y se consideran además aquellos aspectos surgidos debido a cambios organizativos, de entorno, legales o técnicos que afecten a la Política de Seguridad. Se establecen las pautas para comunicar a las partes interesadas los cambios acordados sobre la Política de Seguridad y otras decisiones a considerar.

Son convocados todos los responsables de los departamentos involucrados en la revisión.

4. Informe de Acciones

Se incluirán las decisiones y acciones relacionadas con:

- Mejora de enfoque para manejar la seguridad y sus procesos.
- Mejora de los objetivos de control y controles.
- Mejora de la asignación de recursos y/o responsabilidades.

5. Ejecución de Acciones y Seguimiento

Se llevan a cabo las acciones acordadas para asegurar que la Política de Seguridad cumple con los requerimientos establecidos. El Responsable de Seguridad realiza el seguimiento adecuado para que dichas acciones se realicen en los plazos y en los términos establecidos y aprobados por el Comité de Seguridad. Se procede a comunicar los cambios y acciones a realizar a las partes interesadas.

6. Validación Final de la Política de Seguridad

Reunión para verificar la validez de la política tras las acciones o decisiones consideradas y/o ejecutadas.

7. Aprobación de Política de Seguridad

Se procede a la aprobación de la Política de Seguridad por parte del Comité una vez revisados los cambios y tomadas las decisiones. Se mantiene un registro de revisión gerencial a partir del que se obtiene la aprobación de la Política revisada.

El periodo de revisión es anual y se realizará previo a la auditoría anual.

6. VIOLACIÓN DE LA POLÍTICA DE SEGURIDAD

Innovasur podrá tomar las medidas adecuadas contra toda aquella persona que contravenga la Política de Seguridad y que derive en una amenaza en el negocio y/o mantenimiento de la actividad o en una violación de las normativas legales y/o acuerdos contractuales a los que Innovasur estuviese obligado.

El nivel y grado de las medidas dependerá de la naturaleza, intencionalidad y alcance de lo contravenido.

Tanto en el caso de relaciones laborales como de otra naturaleza, Innovasur se reserva el derecho de emprender acciones legales, independientemente de la rescisión de la relación contractual, en función del daño causado a la Entidad.

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 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 en la intranet de Innovasur.

8. FORMACIÓN Y CONCIENCIACIÓN

Con carácter anual se realizará una acción de formación y concienciación en materia de seguridad.

El objetivo de la acción formativa y de concienciación es doble:

- 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.

9. GESTIÓN DE RIESGOS

Los servicios e infraestructuras bajo el alcance de la presente Política deberán estar sometidos a un análisis de riesgos para orientar las medidas de protección para minimizar los mismos.

Como metodología base para la realización de los análisis de riesgos se utilizará Magerit.

Se utilizarán, como punto de partida, el catálogo de amenazas de seguridad previsto en la metodología.

El análisis se realizará:

- Regularmente, una vez al año.
- Cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.

De acuerdo con la escala de riesgos de la metodología Magerit, el nivel de riesgo deberá situarse por debajo del nivel ALTO para considerarse de forma automática como aceptable (el riesgo residual máximo debe ser MEDIO). Valores de riesgo residual mayores a MEDIO deberán ser aceptados explícitamente por el Comité de Seguridad, previa justificación de la conveniencia de su aceptación.

Para los valores de riesgo residual que no sean aceptables se deberá elaborar el correspondiente Plan de Mejora que permita llevar los valores de riesgo a valores aceptables.

10. DATOS PERSONALES

Innovasur solo 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.

11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Esta Política de Seguridad se desarrollará mediante la elaboración de otras políticas o normativas de seguridad que aborden aspectos específicos. A raíz de dichas políticas y normativas se podrán desarrollar procedimientos que describan la forma de llevarlas a cabo.

12. 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.

13. APROBACIÓN Y ENTRADA EN VIGOR

La presente Política de Seguridad de la Información será aprobada por 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/ENS de la entidad.