Inarsys S.L.

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (Esquema Nacional de Seguridad-ENS)


USO CONFIDENCIAL

# HOJA DE INFORMACIÓN GENERAL

***CONTROL DOCUMENTAL***

| | |
|---|---|
| **PROYECTO** | ENS |
| **DESTINATARIO:** | Toda la Organización de Inarsys S.L. |
| **TITULO:** | POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. |
| **REFERENCIA:** | D-2023-ENS-PIN-008 |
| **VERSIÓN:** | 2.0 |
| **AUTOR:** | Inarsys. |

## *ESTADO FORMAL:*

| Preparado por: | Aprobado por: |
|---|---|
| NOMBRE:<br>Inarsys<br>FECHA: 01/04/2024 | NOMBRE:<br>Pedro Romera Murillo<br>Luis Sanchez Fernández<br>Fernando Gallo Nieto<br>FECHA: 01/04/2024 |

# Índice

# 1 OBJETO

*El objeto de este documento es definir la política de Inarsys para la seguridad de la información.*

# 2 ALCANCE

*Este documento aplica a todas las partes interesadas y activos de información de Inarsys. El alcance del sistema de gestión de seguridad de la información es el siguiente:*

> *"Los sistemas de información que dan soporte a las actividades profesionales de consultoría, arquitectura e ingeniería de infraestructuras de tecnología de la información y comunicaciones".*

# 3 MARCO NORMATIVO

*Inarsys está sujeta a las siguientes leyes, reglamentos y otra normativa, nacional e internacional en materia de seguridad de la información:*

- *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad*
- *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 (Reglamento general de protección de datos)*
- *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*
- *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 (vigente en aquellos artículos que no contradigan el RGPD)*
- *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*
- *Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual*

# 4 DESARROLLO

*Inarsys depende de los activos de información para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad, autenticidad y trazabilidad de la información tratada o los servicios prestados.*

*Los objetivos de la organización de seguridad de la información de Inarsys son:*

- *Garantizar que no se producen accesos no autorizados.*
- *Prestar unos servicios que cumplan los requisitos de disponibilidad.*
- *Preservar la integridad de la información.*
- *Garantizar el no repudio, cuando se requiera.*
- *Disponer de suficientes eventos para garantizar la trazabilidad requerida.*

## *4.1 PREVENCIÓN*

*Las personas deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad de la información.*

*Para ello, Inarsys debe implementar las medidas mínimas de seguridad de la información determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de la información de todas las personas, deben estar claramente definidos y documentados.*

*Para garantizar el cumplimiento de la política, Inarsys debe:*

- *Autorizar los activos de información antes de entrar en operación.*
- *Evaluar regularmente la seguridad de la información, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.*
- *Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.*

## *4.2 DETECCIÓN*

*Dado que los servicios y los activos se pueden degradar rápidamente debido a incidentes de seguridad de la información, que van desde una simple desaceleración hasta su detención, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.*

*La monitorización es especialmente relevante cuando se establecen líneas de defensa.*

*Se han establecido mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.*

## *4.3 RESPUESTA*

*Inarsys ha:*

- *Establecido los mecanismos para responder eficazmente a los incidentes de seguridad de la información.*
- *Designado un punto de contacto para las comunicaciones con respecto a incidentes de seguridad de la información detectados.*

- *Establecidos protocolos para el intercambio de información relacionada con el incidente.*

### *4.4 RECUPERACIÓN*

*Para garantizar la disponibilidad de los servicios críticos, Inarsys ha desarrollado planes de continuidad de los servicios como parte de su plan general de continuidad de negocio y actividades de recuperación.*

## 5 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

*En Inarsys los roles relevantes en materia de seguridad de la información son los siguientes:*

- *El comité de seguridad de la información es la máxima autoridad y responsable en materia de seguridad de la información de Inarsys, coordina la gestión del cumplimiento de todos los requisitos de cliente, legales y reglamentarios en esta materia, y gestiona los potenciales conflictos. En el caso de Inarsys está formado por los Responsables de Tecnología e Innovación, Arquitectura y Transformación, y Desarrollo de Negocio.*
- *El responsable de la información determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS (categorización de nivel bajo, medio o alto en las dimensiones de seguridad de la información). En el caso de Inarsys es el Responsable de Arquitectura y Transformación.*
- *El responsable del servicio determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS (categorización de nivel bajo, medio o alto en las dimensiones de seguridad de la información). En el caso de Inarsys es el Responsable de Tecnología e Innovación.*
- *El responsable de seguridad determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios, siendo jerárquicamente independiente del responsable del sistema. En el caso de Inarsys es el Responsable de Tecnología e Innovación.*
- *El 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. En el caso de Inarsys es el Responsable de Arquitectura y Transformación.*

*El procedimiento para la designación y renovación de los roles o funciones de seguridad se realiza a través de reuniones del Comité de Seguridad de la Información, de las cuales se dispondrá de las correspondientes actas, ver documento "ACTA DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DE INARSYS firmado.pdf".*

*El punto de contacto (POC) de Inarsys es la dirección de correo electrónico seguridad@inarsys.com.*

# 6 REVISIÓN, APROBACIÓN Y COMUNICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

*El comité de seguridad de la información aprueba la política de seguridad de la información, y la revisa al menos anualmente.*

*La política de seguridad de la información está publicada en la página Web corporativa.*

# 7 DATOS DE CARÁCTER PERSONAL

*Inarsys trata datos de carácter personal conforme a la legislación vigente en materia de protección de datos de carácter personal.*

# 8 ANÁLISIS Y GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

De todos los activos de información de Inarsys se ha realizado un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

*Este análisis se revisa y, si procede actualiza:*

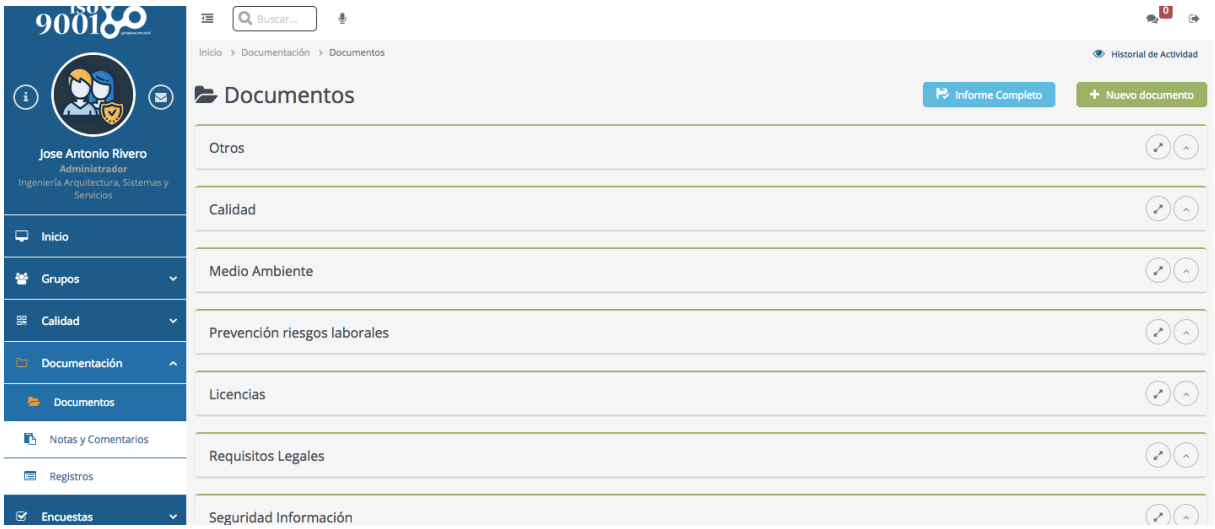
- *Regularmente, al menos una vez al año.*
- *Cuando cambia la información manejada.*
- *Cuando cambian los servicios prestados.*
- *Cuando ocurre un incidente grave de seguridad de la información.*
- *Cuando se reportan vulnerabilidades graves.*

# 9 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

*Esta política de seguridad de la información se desarrolla en otras políticas más concretas, normativas, procedimientos, que se estructuran, gestionan y controlan su acceso de acuerdo al procedimiento de control de la documentación siguiente:*

- *Todos los documentos del Esquema Nacional de Seguridad (ENS) son elaborados por el Responsable del Sistema en colaboración con el Responsable de Calidad. Los documentos actualizados se relacionan en la aplicación informática **ISO 9001**, sección "Documentación".*

  *Se encuentran identificados por el código, nombre y número de edición (cuando se emiten documentos por primera vez, Nº edición = 1).*




- *La codificación de documentos del ENS se realiza de la siguiente manera:*
  *Documentación Referente al Negocio*
  ***NEG***
  *Documentación Referente a Normativa Interna*
  ***NIN***
  *Documentación Referente a Instrucciones Internas*
  ***INT***
  *Documentación Referente a Política Interna*
  ***PIN***
  *Documentación Referente a Registro de Revisiones*
  ***REG***

  *La documentación de cada uno de los capítulos anteriores se numera con 3 dígitos desde el 001 y siguiendo de forma correlativa dentro de cada uno de los capítulos.*

## 10 OBLIGACIONES DE LAS PERSONAS

*Todos las personas propias y subcontratadas, de Inarsys tienen la obligación de conocer y cumplir esta política de seguridad de la información de la información y el resto de documentación que la desarrolla.*

*Todas las personas son concienciadas regularmente, en particular a los de nueva incorporación.*

*Las personas con responsabilidad en el uso, operación o administración de los sistemas de información recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.*

## 11 TERCERAS PARTES

*Cuando Inarsys presta servicios o trate información de otras organizaciones:*

- *Se les hace partícipes de esta política de seguridad de la información.*
- *Se establecen canales para reporte y coordinación al comité de seguridad de la información.*
- *Se establecen procedimientos de actuación para la reacción ante incidentes de seguridad de la información de seguridad.*

*Cuando Inarsys utiliza servicios de terceros o ceda información a terceros:*

- *Se les hace partícipes de esta política y de la normativa de seguridad de la información que ataña a dichos servicios o información.*
- *Dicha tercera parte queda sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.*
- *Se establecen procedimientos específicos de reporte y resolución de incidencias.*
- *Se requiere que el personal de terceros esté adecuadamente concienciado en materia de seguridad de la información, al menos al mismo nivel que el establecido en esta política.*

*Cuando algún aspecto de la política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requiere un informe del responsable de seguridad de la información que precisa los riesgos en que se incurre y la forma de tratarlos. Se requiere la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.*

## 12 HISTÓRICO DE CAMBIOS

| Edición | Fecha | Cambio Realizado/ Motivo |
|---|---|---|
| 1.0 | 17/05/2023 | Edición Inicial. |
| 2.0 | 01/04/2024 | Cambios referentes a misión y objetivo de la organización de seguridad (2,4), procedimiento de designación de roles (5) y estructura de la documentación de seguridad (9). |

*Firmado:*

01109635T PEDRO LUIS ROMERA MURILLO (R: B86181286)

Firmado digitalmente por 01109635T PEDRO LUIS ROMERA MURILLO (R: B86181286)
Fecha: 2024.04.01 12:21:06 +02'00'

*Pedro Romera Murillo*