SI01 – Política de Seguridad de la Información

Versión 4 – 20/01/2022

Documento	
Nombre	SI01 – Política de Seguridad de la Información
Versión	4
Autor	RSI – Responsable de Seguridad de la Información
Órgano de aprobación	CSI – Comité de Seguridad de la Información
Fecha de aprobación	20/01/2022

Control de Versiones				
Versión	***Autor***	***Aprobación***	***Fecha***	***Cambios realizados***
1	LP	CSI	20/10/2021	Versión inicial
2	LP	CSI	23/12/2021	Añadir el Flujo de Información del sistema
3	LP	CSI	3/01/2022	Procedimiento de Gestión de Riesgos
4	LP	CSI	20/01/2022	requisitos para nuevos sistemas de información

Domicilio
Compromiso de Caspe,
Nº 1 Pta. 2
46007 VALENCIA
Teléfono
963 410 406
Fax
963 416 304
E mail
admon@ival.com
Web
www.ival.com

Índice

Política de Seguridad de la Información

1. Introducción

1.1 Misión de IVAL informática

IVAL informática es una empresa especializada en la informatización de la gestión de las Administraciones Públicas, a las que presta los siguientes servicios:

- Consultoría para la mejora e informatización de su gestión.
- Diseño y desarrollo de aplicaciones de gestión pública.
- Implantación y puesta en marcha de estas aplicaciones.
- Asistencia técnica a los usuarios de estas aplicaciones.
- Realización de trabajos para los clientes utilizando estas aplicaciones.

1.2. Alcance

El Alcance de la presente Política de Seguridad de la Información es:

Los sistemas de información que dan soporte al servicio de gestión de soporte a los clientes de nuestra aplicación *panGEA* – *Gestión integrada para las Administraciones públicas*.

2. Marco normativo

El marco normativo que rige la actividad de ***IVAL informática*** en el ámbito de la Seguridad de la Información está establecido por las siguientes normas y regulaciones:

- LSSICE: Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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.
- ISO 27001: Norma española UNE-ISO/IEC 27001 – Sistemas de Gestión de Seguridad de la Información (SGSI).

3. Política de Seguridad de la Información

3.1. Objetivo de la Política de Seguridad de Información

IVAL informática depende por completo de sus Sistemas de Información para poder prestar servicio a sus clientes.

Por lo tanto, estos Sistemas de Información deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a integridad y la confidencialidad de la información tratada y a la disponibilidad de los servicios prestados.

El **objetivo principal** de la presente Política es definir los principios y las reglas básicas que se van a seguir en ***IVAL informática*** para **garantizar la seguridad de la información** que se maneja en la empresa y minimizar los posibles riesgos que podría provocar su gestión ineficaz para, de esta forma, **garantizar la prestación continuada de los servicios** que ofrecemos a nuestros clientes.

3.2. Principios de la Política de Seguridad

IVAL informática establece los siguientes principios básicos como directrices fundamentales de la seguridad de la información que han de tenerse presentes en toda actividad relacionada con el tratamiento de información:

- Alcance estratégico:

  La seguridad de la información deberá contar con el compromiso y apoyo de todos los niveles directivos de ***IVAL informática*** de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la empresa para conformar un marco de trabajo coherente y eficaz.

- Seguridad integral:

  La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos.

  Por ello cuando se establezcan los requisitos para nuevos sistemas de información o para mejorar los ya existentes, se deberán incluir entre ellos los requisitos relacionados con la seguridad de la información.

- Concienciación y formación:

  Se prestará la máxima atención a la concienciación y formación en seguridad de la información de todas las personas que intervienen en el proceso de la información, para que ni la ignorancia, ni la falta de organización y coordinación sean fuentes de riesgo para la seguridad de la información.

- Gestión de riesgos:

  El análisis y gestión de riesgos será una parte esencial del proceso de seguridad de la información.

  La gestión de riesgos mediante las oportunas medidas de seguridad permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.

- Proporcionalidad:

  El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

- Mejora continua:

  Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

- Seguridad por defecto:

  Los sistemas de información deberán configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

3.3. Comunicación de la Política de Seguridad de la Información

La presente Política de Seguridad de la Información de ***IVAL informática*** se publicará para su conocimiento por todas las partes interesadas:

- En la página web corporativa de la empresa: ***www.ival.com***
- En la página web de entrada al servicio de soporte: ***soporte.ival.com***
- En la página principal de todos los módulos de la aplicación ***panGEA***

4. Compromiso de la Dirección

La Dirección de ***IVAL informática***, consciente de la importancia de la seguridad de la información para conseguir llevar a cabo con éxito sus objetivos de negocio, se compromete a:

- Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
- Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Impulsar la concienciación y formación en Seguridad de la Información entre todos los empleados.
- Exigir el cumplimiento de la presente Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- Considerar los riesgos de seguridad de la información en la toma de decisiones.

5. Organización de seguridad de la Información

5.1. Definición de comités y roles unipersonales

La organización de Seguridad de la Información de ***IVAL informática*** se ha establecido siguiendo las recomendaciones de las Guías de Seguridad de las TIC del CNC:

- CCN-STIC-402 Organización y Gestión para la Seguridad de los Sistemas TIC

  Anexo C – Organizaciones medianas
- CCN-STIC-801 ENS – Responsabilidades y Funciones

  Anexo B – Estructuras posibles de implantación – Estructura intermedia

Por lo tanto, la organización de Seguridad de la Información de ***IVAL informática*** se ha establecido a tres niveles:

- **Alta Dirección:**
  - **CSI – Comité de Seguridad de la Información.**
    Está formado por el Consejo de Administración de la sociedad.
- **Supervisión:**
  - **RSI – Responsable de Seguridad de la Información.**
    El RSI es el Gerente de la empresa.
- **Operación:**
  - **ASIST – Administrador del Sistema de Información.**
    El ASIST es el Administrador del Sistema de Información que constituye el Alcance de esta Política de Seguridad de la Información.
  - **Usuarios del Sistema de Información.**
    Usuarios internos del Sistema de Información que constituye el Alcance de esta Política de Seguridad de la Información

5.2. Funciones y Responsabilidades

5.2.1. CSI – Comité de Seguridad de la Información

Sus funciones son las siguientes:

- Coordinar todas las funciones y todas las actividades relacionadas con la Seguridad de la Información en la empresa.
- Velar por el cumplimiento de la normativa legal, regulatoria y sectorial.
- Velar por el alineamiento de las actividades de seguridad con los objetivos de la empresa.
- Aprobar la “Política de Seguridad de la Información” y los demás documentos del Sistema de Seguridad de la Información de la empresa.
- Revisar su cumplimiento recabando al “Responsable de Seguridad de la Información” informes periódicos sobre el estado de seguridad del sistema y los posibles incidentes que se puedan producir.

5.2.2. RSI – Responsable de Seguridad de la Información

Sus funciones son las siguientes:

- Actuar como Secretario del “Comité de Seguridad de la Información”.
- Convocar las reuniones del “Comité de Seguridad de la Información” preparando el orden del día y recopilando la información pertinente para su discusión.
- Elaborar los documentos del Sistema de Seguridad de la Información de la empresa y presentarlos al “Comité de Seguridad de la Información” para su aprobación.
- Verificar y supervisar su cumplimiento.

- Estar al tanto de los cambios normativos que afecten a la empresa, informarse de sus consecuencias para las actividades de la empresa y proponer al “Comité de Seguridad de la Información” las medidas oportunas.
- Tomar las decisiones día a día entre las reuniones del “Comité de Seguridad de la Información” velando por la unidad de acción y la coordinación de actuaciones, en especial en caso de producirse incidencias.
- Ser el interlocutor con otras organizaciones en materias referidas a la Seguridad de la Información.
- Coordinar la respuesta ante incidentes de Seguridad de la Información que desborden los casos previstos y procedimentados, y la investigación forense relacionada con incidentes que se consideren relevantes.

5.2.3. ASIST – Administrador del Sistema de Información

Sus funciones son las siguientes:

- Estar al tanto de los cambios en la tecnología de la información y el entorno de la empresa que afecten a ésta, informarse de sus consecuencias para las actividades de Seguridad de la Información que se realizan, alertar de ellas al “RSI Responsable de Seguridad de la Información” y proponer las medidas oportunas de adecuación al nuevo marco.
- Responsabilizarse de la correcta ejecución de las instrucciones emanadas del “Comité Responsable del Sistema de Información” mediante la transmisión de instrucciones a los usuarios del Sistema de Información.
- Responsabilizarse de que se realicen regularmente verificaciones de seguridad de la información según el “Plan de Verificaciones de la Seguridad de la Información” y presentar su resultado al “RSI Responsable de Seguridad de la Información”.
- Proponer al “RSI Responsable de Seguridad de la Información” medidas correctoras si detectara algún incumplimiento, y responsabilizarse de que sean aplicadas.
- Elaborar los requisitos de formación y calificación de los usuarios del Sistema de Información desde el punto de vista de la Seguridad de la Información.

5.2.5. Agentes

Los Agentes son los usuarios internos del Sistema de Información de la empresa.

Sus funciones son las siguientes:

- Realizar la operación diaria de los servicios de seguridad de la información que haya implantado el Administrador de la Seguridad de la Información.
- Ejecutar los procedimientos que les competan dentro de la actividad rutinaria de la empresa.
- Ejecutar los procedimientos que les competan para la resolución de los incidentes de seguridad que perciban durante la realización de sus tareas.

- Comunicar al Administrador del Sistema de Información todas las incidencias de seguridad de la información que se produzcan y todas las vulnerabilidades del sistema de información que detecten o de las que tengan constancia.

5.2.6. Resumen

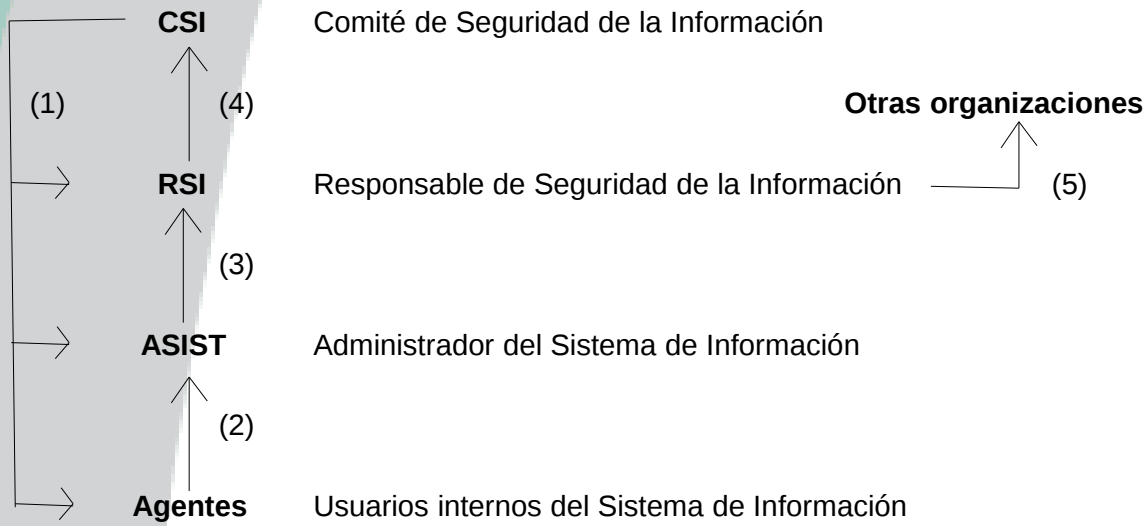
Órganos para la Seguridad de la Información			
Nivel	***Organización***		
	Seguridad de la Información		***Operativa***
Alta Dirección	**CSI**	Comité de Seguridad de la Información	Consejo de Administración
Supervisión	**RSI**	Responsable de Seguridad de la Información	Gerente
Operativo	**ASIST**	Administrador del Sistema de Información	Administrador del Sistema de Información
	Agentes		Usuarios internos del Sistema de Información

5.3. Documentos del Sistema de Seguridad de la Información

Documentos del Sistema de Seguridad de la Información		
Documento	***Elaborado por***	***Aprobado por***
Política de Seguridad de la Información	RSI	CSI
Plan de Concienciación y Formación del Personal	RSI	CSI
Plan de Revisiones de la Seguridad de la Información	RSI	CSI
Procedimientos de Seguridad de la Información	RSI	CSI
Documento de Seguridad de datos de carácter personal	N/A	N/A
Informes periódicos sobre el estado de la Seguridad de la Información	RSI	CSI
Informes sobre incidentes de Seguridad de la Información especialmente graves y desastres	RSI	CSI
Procedimiento de Categorización del Sistema de Información	RSI	CSI
Documento de Categorización del Sistema de Información	RSI	CSI
Análisis de Activos del Sistema, Amenazas, Medidas de Seguridad y Riesgos	RSI	CSI

Procedimientos de utilización del Sistema de Información	RSI	CSI
Requisitos de formación y calificación de los administradores y usuarios del Sistema de Información	RSI	CSI

5.4. Flujo de Información del Sistema de Seguridad de la Información



(1) Documentos del Sistema de Seguridad de la Información

(2) Comunicación de incidencias y vulnerabilidades del sistema

(3) Informes sobre incidencias y vulnerabilidades de seguridad que afecten a los activos esenciales del sistema (informaciones y servicios)

(4) Informes sobre:
- Estado de la seguridad del sistema
- Incidentes de seguridad de la información que se hayan producido
- Actuaciones realizadas en materia de seguridad de la información

(5) Intercambio de información con otras organizaciones sobre Seguridad de la Información

5.5. Mecanismos de coordinación

La coordinación de la Seguridad de la Información será **responsabilidad del *RSI* – *Responsable de Seguridad de la Información***.

5.6 Procedimientos de designación de personas

La designación de las personas que constituyan los comités y ejerzan los roles unipersonales relacionados con la Seguridad de la Información serán **designados por el Consejo de Administración** de la sociedad.

6. Concienciación y formación

Los usuarios de los Sistemas de Información de una organización juegan un papel fundamental en el mantenimiento de su seguridad ya que en la mayoría de los casos constituyen, voluntariamente o involuntariamente, su principal amenaza.

Por lo tanto ***IVAL informática***, considera que uno de los objetivos más importantes de la presente Política de Seguridad de la Información es lograr la plena conciencia de todos sus miembros respecto a que la seguridad de la información les conscierne a todos ellos y afecta a todas las actividades que se realicen en la empresa.

Para conseguirlo, el *RSI – Responsable de Seguridad de la Información* elaborará un "**Procedimiento de Concienciación y Formación del personal en Seguridad de la Información**" que presentará al *CSI – Comité de Seguridad de la Información* para su aprobación y en el que se deberá establecer, entre otros aspectos, que los usuarios de los sistemas de información que constituyen el alcance de la presente Política deberán estar:

- Informados de su obligación de obrar con diligencia con respecto a la información, debiéndose asegurar que dicha información no caiga en poder de empleados o terceros no autorizados.
- Informados de las actualizaciones de las políticas y procedimientos de seguridad en los que se vean afectados y de las amenazas existentes.
- Informados de sus obligaciones y responsabilidades en materia de Seguridad de la Información.
- Formados en relación a la gestión de mecanismos de identificación y al procedimiento de gestión de incidentes.

7. Gestión de riesgos

El análisis y gestión de riesgos es una parte esencial del proceso de Seguridad de la Información pues permite mantener un entorno controlado para su utilización minimizando los riesgos previsibles hasta niveles que se consideren aceptables, mediante el despliegue de medidas de seguridad.

Para conseguirlo, el R*SI – Responsable de Seguridad de la Información* elaborará un *Procedimiento de Gestión de Riesgos* que deberá ser aprobado por el *CSI – Comité de Seguridad de la Información.*

8. Clasificación de la Información

La información manejada por un sistema de información se puede clasificar en tres categorías:

- Confidencial:

  Su revelación supondría un grave daño:
  - Supondría una ventaja comercial desproporcionada para la competencia.
  - Supondría un grave quebranto económico.
  - Podría quebrar la capacidad de operar de la Organización.
  - Supondría un serio daño a la imagen de la Organización

- Difusión limitada

  Su revelación causaría daños indeseables:

  - Supondría un ventaja comercial para la competencia.
  - Supondría un quebranto económico.
  - Dañaría significativamente a la capacidad de operar de la Organización.
  - Supondría un cierto daño a la imagen de la Organización.
  - Supondría un incumplimiento de las obligaciones de confidencialidad adquiridas por la Organización con respecto de terceros.
  - Supondría un incumplimiento de obligaciones legales (ejemplos: datos de carácter personal, salarios, acuerdos con clientes y proveedores, …)

- Sin clasificar

  Su revelación no supondría un gran perjuicio, aunque pudiera ser embarazosa.

  En este capítulo se suele dejar la información interna que no es pública, y a la que pueden acceder todos los miembros de la Organización (ejemplos: listín telefónico, guías de procedimientos internos, borradores de documentos, ...)

Los Sistemas de Información que forman el alcance de la presente Política:

- **No manejan ningún dato de carácter personal**.
- Además, **toda la información** que manejan **pertenece a la categoría "Sin clasificar"** pues su revelación no supondría un gran perjuicio para la empresa.

9. Proceso de revisión de la Política de Seguridad

La Política de Seguridad de la Información de ***IVAL informática*** la ha elaborado el *RSI – Responsable de Seguridad de la Información* y la ha aprobado el *CSI – Comité de Seguridad de la Información*.

Esta Política **se revisará anualmente** por el *RSI – Responsable de Seguridad de la Información*, quien presentará la nueva versión revisada al *CSI – Comité de Seguridad de la Información* para que la apruebe.

No obstante, si tuvieran lugar cambios relevantes en la empresa o se identificaran cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal o regulatorio, esta política se revisará siempre que se considere necesario para asegurar que permanezca adaptada en todo momento a la situación de la empresa.

10. Obligaciones del personal

Los miembros de ***IVAL informática*** tienen las siguientes obligaciones:

- Conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad de la Información de la empresa.
- Realizar las actividades de concienciación y de formación que les afecten, de las especificadas en el Plan de Formación de la Seguridad de la Información de la empresa.

- Suscribir un Contrato de Confidencialidad comprometiéndose a guardar secreto respecto de toda la información confidencial a la que pueda tener acceso como consecuencia de la prestación de sus servicios laborales.

11. Relaciones con Terceras Partes

11.1. Clientes

- Se establecerán canales para la coordinación de sus Políticas de Seguridad de la Información propias con la de ***IVAL informática***.
- Se establecerán canales para la mutua comunicación de las vulnerabilidades que se detecten y de las incidencias que se puedan producir.

11.2. Proveedores de Servicios de Información

- Se garantizará que su personal esté adecuadamente concienciado en materia de seguridad de la información, al menos al mismo nivel que el establecido en la presente Política.
- Se establecerán canales para la coordinación de sus Políticas de Seguridad de la Información propias con la de ***IVAL informática***
- Se establecerán canales para la mutua comunicación de las vulnerabilidades que se detecten y de las incidencias que se puedan producir.

11.2.1 Contrato de Tratamiento de datos

- **Proveedores certificados.**

  Los proveedores de servicios de información que estén certificados ***ISO27001*** o ***ENS Media*** se considerarán proveedores de confianza por lo que no será necesario suscribir con ellos ningún contrato de tratamiento de datos.

- **Proveedores no certificados.**

  Los proveedores de servicios de información que no estén certificados ***ISO27001*** ni ***ENS Media*** no se considerarán proveedores de confianza por lo que será necesario suscribir con ellos un contrato de tratamiento de datos.

11.3. Imposibilidad de cumplimiento por terceras partes

Cuando una tercera parte, cliente o proveedor, no pueda satisfacer alguna de las condiciones indicadas, será necesario que el *RSI – Responsable de Seguridad de la Información* elabore un informe precisando los los riesgos en que se incurre y la forma de tratarlos, que deberá ser aprobado por el *CSI – Comité de Seguridad de la Información*.