SI01 – Política de Seguridad de la Información

Versión 7 – 7/04/2022

Documento	
Nombre	SI01 – Política de Seguridad de la Información
Versión	7
Autor	RSI – Responsable de Seguridad de la Información
Órgano de aprobación	CSI – Comité de Seguridad de la Información
Fecha de aprobación	7/04/2022

Control de Versiones				
Versión	**Autor**	**Aprobación**	**Fecha**	**Cambios realizados**
1	RSI	CSI	20/10/2021	Versión inicial
2	RSI	CSI	23/12/2021	Añadir el Flujo de Información del sistema
3	RSI	CSI	3/01/2022	Procedimiento de Gestión de Riesgos
4	RSI	CSI	20/01/2022	Requisitos para nuevos sistemas de información
5	RSI	CSI	14/02/2022	Cambios derivados de la auditoría interna de 21/01/22
6	RSI	CSI	9/03/2022	Cambios derivados del estudio documental de 28/02/22
7	RSI	CSI	7/04/2022	Cambios derivados de la auditoría de AENOR de 14/03/22

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 sistema de gestión de peticiones e incidencias de los clientes de la 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.
- RGPD: 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.
- 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.
- ENS: 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.
- ISO 27001: Norma española UNE-ISO/IEC 27001 – Sistemas de Gestión de Seguridad de la Información (SGSI).

3. Objetivo de la Política de Seguridad de la Informarción

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 la Confidencialidad, Integridad, Autenticidad y Trazabilidad de la información tratada y a la Disponibilidad de los servicios prestados:

- **Confidencialidad de la información.**

  Consecuencias que tendría el acceso a la información por parte de personas que no estén autorizadas, o que no necesiten, acceder a ella.

- **Integridad de los datos.**

  Consecuencias que tendría la modificación de los datos por parte de personas que no estén autorizadas a modificarlos.

- **Autenticidad de la información y de los actores.**

  Consecuencias que tendría el que una información no sea auténtica o no se pueda garantizar la fuente de la que procede, o que una entidad no sea quien dice ser.

- **Trazabilidad del uso del servicio.**

  Consecuencias que tendría el no poder comprobar a posteriori que persona, o sistema interconectado, ha accedido o modificado la información, o que las actuaciones de una entidad no puedan ser imputadas exclusivamente a dicha entidad.

- **Disponibilidad de los servicios.**

  Consecuencias que tendría el que una persona, o un sistema interconectado, no pudiera usar el activo cuando lo necesite, dentro del período de acceso establecido y anunciado.

El **objetivo principal** de la presente *Política de Seguridad de la Información* 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.

4. Principios de la Política de Seguridad

IVAL informática establece los siguientes principios como directrices 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.

- **Organización e implantación del proceso de seguridad.**

  La seguridad de la información compromete a todos los miembros de la organización.

  La presente *Política de Seguridad de la Información* establece los responsables de de velar por su cumplimiento y se hará pública para que sea conocida por todos los miembros de la organización y por todas las partes interesadas.

- **Análisis y gestión de los riesgos.**

  La gestión de la Seguridad de la Información se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema, utilizando la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información ***MAGERIT v.3***.

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

  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.

- **Gestión de personal.**

  Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad.

  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.

  Las actuaciones de todo el personal serán supervisadas para verificar que se siguen los procedimientos establecidos.

  El personal relacionado con la información y los sistemas, ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.

  El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad.

  Cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

- **Profesionalidad.**

  La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

  Todo el personal recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información que utilicen.

Se exigirá, de manera objetiva y no discriminatoria, que los proveedores de servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

- **Autorización y control de los accesos.**

  El acceso a los sistemas de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

- **Protección de las instalaciones.**

  Los sistemas se instalarán en áreas separadas y cerradas, dotadas de un procedimiento de control de llaves y de accesos.

- **Adquisición de productos.**

  En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del *Responsable de Seguridad de la Información*.

- **Seguridad por defecto.**

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

  El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

  Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados.

  En los sistemas de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

  El uso ordinario de los sistemas ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

- **Integridad y actualización del sistema.**

  Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

  Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista de su estado de seguridad.

- **Protección de la información almacenada y en tránsito.**

  Se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros (equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil, ...)

  Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica manejada por el sistema

deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren.

- **Prevención ante otros sistemas de información interconectados.**

  El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas.

  En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

- **Registro de actividad.**

  Se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

- **Incidentes de seguridad.**

  Se establecerá un sistema de detección y reacción frente a código dañino.

  Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información que cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

- **Continuidad de la actividad.**

  Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

- **Mejora continua del proceso de seguridad.**

  El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

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

5. 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***

6. 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.

7. Organización de seguridad de la Información

7.1. 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 B – Pequeñas organizaciones:

  Dispondrán de un único Comité de Seguridad.

  El Responsable de Seguridad Corporativa asumirá todas las responsabilidades.

- CCN-STIC-801 ENS – Responsabilidades y Funciones

  Anexo B – Estructuras posibles de implantación – Estructura mínima:

  Las responsabilidades pueden implementarse en dos roles:

  - Gobierno y Supervisión.

    Una figura integrando las siguientes funciones:

    Responsable del Tratamiento (si hay datos de carácter personal).

    Responsable de la Información.

    Responsable del Servicio.

    Responsable de la Seguridad.

    Delegado de Protección de Datos.

  - Operación.

    Una figura, reportando a Dirección, e integrando las siguientes funciones:

    Responsable del Sistema.

    Administrador de Seguridad.

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

- **Gobierno y Supervición:**
  - **CSI – Comité de Seguridad de la Información.**

    Está formado por los miembros del Consejo de Administración de la sociedad.

    Uno de sus miembros, el Gerente de la empresa, ejercerá las funciones de **RSI – Responsable de Seguridad de la Información**.
- **Operación:**
  - **ASIST – Administrador del Sistema de Información.**

    El ASIST es el Administrador de los Sistemas de Información de la empresa.
  - **Usuarios del Sistema de Información.**

    Usuarios internos del Sistema de Información que constituye el Alcance de esta Política de Seguridad de la Información (Agentes).

7.2. Funciones y Responsabilidades

7.2.1. 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.

7.2.2. RSI – Responsable de Seguridad de la Información

Sus funciones son las siguientes:

- Actuar como Secretario del “CSI – Comité de Seguridad de la Información”.
- Convocar las reuniones del “CSI – Comité de Seguridad de la Información” preparando el orden del día y recopilando la información pertinente para su discusión.
- Desempeñar las funciones de:
  - Responsable de la Información

    Establecer los requisitos en materia de seguridad (niveles de seguridad) de la información tratada por el sistema.

- Responsable del Servicio

  Establecer los requisitos en materia de seguridad (niveles de seguridad) del servicio.

- Delegado de Protección de Datos

  Comprobar el cumplimiento de la LOPDGDD.

- Responsable del Tratamiento de datos de carácter personal

- Evaluar los riesgos que pueden derivarse del tratamiento de datos personales y adoptar las medidas necesarias que garanticen su seguridad.

- Elaborar los documentos del Sistema de Seguridad de la Información de la empresa y presentarlos al "CSI – Comité de Seguridad de la Información" para su aprobación.
- Verificar y supervisar su cumplimiento.
- 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.
- Realizar regularmente las verificaciones de seguridad de la información según el "Plan de Verificaciones de la Seguridad de la Información" y presentar su resultado al "CSI – Comité de Seguridad de la Información".
- 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 "CSI – 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.

7.2.3. 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 "CSI – Comité de Seguridad de la Información" mediante la transmisión de instrucciones a los usuarios del Sistema de Información.
- Proponer al "RSI – Responsable de Seguridad de la Información" medidas correctoras si detectara algún incumplimiento, y responsabilizarse de que sean aplicadas.

7.2.4. 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.

7.2.5. Resumen

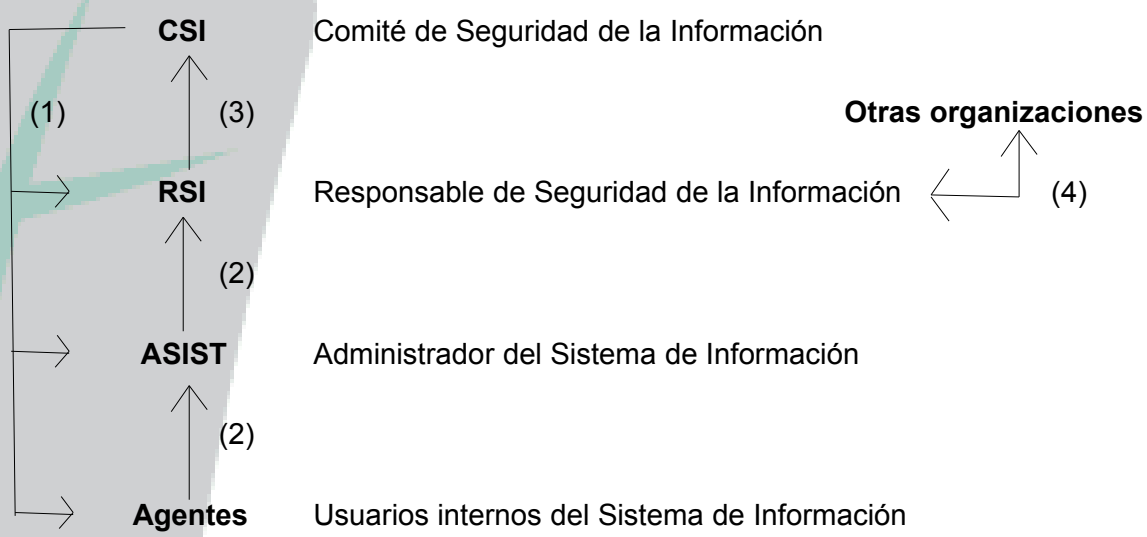
Órganos para la Seguridad de la Información			
Nivel	***Organización***		
	Seguridad de la Información		***Operativa***
Gobierno y Supervisión	**CSI**	Comité de Seguridad de la Información	Consejo de Administración
	RSI	Responsable de Seguridad de la Información	Gerente
Operativo	**ASIST**	Administrador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

7.3. Documentos del Sistema de Seguridad de la Información

Los Documentos de Sistema de Seguridad de la Información se elaborarán siguiendo el procedimiento "PR4201 Elaborar y publicar la documentación interna" del Sistema de Gestión de la Calidad, en el que se establece la Política de Firma electrónica de la empresa.

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

7.4. 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:
- 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

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

7.5. Mecanismos de coordinación y de resolución de conflictos

La coordinación de la Seguridad de la Información y la resolución de los conflictos que ésta pueda suscitar serán **responsabilidad del *RSI – Responsable de Seguridad de la Información***.

7.6. 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.

8. 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.

9. 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.*

10. Clasificación de la Información

La información manejada por un sistema de información se puede clasificar en las siguientes 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, …)
- Pública

  Información publicada por la Organización para su libre acceso por todas las partes interesadas.

Por lo tanto, atendiendo a esta clasificación, **toda la información** que manejan los Sistemas de Información que forman el alcance de la presente Política **pertenece a la categoría "Sin clasificar"** pues, sin ser Pública, su revelación no supondría un gran perjuicio para la Organización.

10.1. Datos de carácter personal

Aunque los Sistemas de Información que forman el alcance de la presente Política no manejan ningún dato de carácter personal y, por lo tanto, no se almacena ningún dato personal en sus bases de datos, en alguna ocasión los usuarios externos pueden adjuntar algún documento a los tickets que abren, que sí que los contenga.

Los datos personales incluidos en estos documentos se tratarán siguiendo las indicaciones establecidas en los documentos *"SI12 – Política de Protección de Datos Personales y Garantía de Derechos Digitales"* y *"SI15 – Registro de las Actividades de Tratamiento de Datos Personales"*.

11. 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.

12. 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.

13. Relaciones con Terceras Partes

13.1. 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.

13.2. 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.
- Se establecerán los requisitos y responsabilidades por ambas partes en relación a la seguridad de la información que se intercambie con los proveedores y al tratamiento que realicen con ella.

  En el caso de que los contratos suscritos con los proveedores para la prestación de Servicios de Información que se les haya contratado no especifiquen estos requisitos y responsabilidades, se suscribirá con ellos un *"Acuerdo de Tratamiento de Datos Personales y Confidencialidad"* adicional al contrato de prestación de servicios, en el que se especifiquen.

13.3. 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*.

LUIS PASCUAL FORNER
Comité Seguridad Información
Motivo: Aprobación
Valencia
07 de abril de 2022