

---

# POLÍTICA ENS

## Política de Seguridad de las Tecnologías de la Información



**Equipo Servicios de Tecnologías de la Información**  
informatica@itainnova.es  
Octubre / 2023



# Índice

01.	APROBACIÓN Y ENTRADA EN VIGOR .....	4
02.	OBJETIVOS Y MISIÓN.....	4
03.	OBJETIVOS DE LA POLÍTICA DE SEGURIDAD.....	5
04.	REVISIÓN DE LA POLÍTICA.....	5
05.	MARCO NORMATIVO .....	6
06.	ÁMBITO DE APLICACIÓN.....	7
07.	PRINCIPIOS DE SEGURIDAD TI.....	7
07.1.	PRINCIPIOS DE SEGURIDAD TI .....	7
07.2.	Requisitos Mínimos de Seguridad .....	8
08.	ORGANIZACIÓN DE LA SEGURIDAD TI .....	10
08.1.	Responsabilidad general .....	11
08.2.	Comisión de Seguridad.....	11
08.3.	Responsable de seguridad TI.....	12
08.4.	Oficina de Seguridad TI .....	12
08.5.	Responsables .....	13
09.	DESARROLLO DE LA POLÍTICA DE SEGURIDAD .....	14
09.1.	Instrumentos del desarrollo .....	14
09.2.	Aprobación de las normativas .....	14
09.3.	Sanciones previstas por incumplimiento .....	14
10.	CONCIENCIACIÓN Y FORMACIÓN.....	15

---

<b>11.</b>	<b>ANÁLISIS Y GESTIÓN DE RIESGOS .....</b>	<b>15</b>
<b>12.</b>	<b>SEGURIDAD DE LA INFORMACIÓN .....</b>	<b>15</b>
<b>13.</b>	<b>DATOS DE CARÁCTER PERSONAL .....</b>	<b>16</b>
<b>14.</b>	<b>OBLIGACIONES DEL PERSONAL .....</b>	<b>16</b>
<b>15.</b>	<b>TERCERAS PARTES .....</b>	<b>16</b>
<b>16.</b>	<b>ANEXO I .....</b>	<b>17</b>
<b>17.</b>	<b>CONTROL DE CAMBIOS.....</b>	<b>18</b>

## 01. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por el comité de Seguridad del Instituto Tecnológico de Aragón, en adelante ITAINNOVA, el 3 de Marzo de 2022. Esta Política de Seguridad de las Tecnologías de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política. La entrada en vigor de la presente Política de Seguridad de la Información de ITAINNOVA supone la derogación de cualquier otra que existiera anteriormente en la organización.

## 02. OBJETIVOS Y MISIÓN DE ITAINNOVA

**Misión:** Centro de promoción de la investigación y el desarrollo, con arreglo al interés general, orientando sus actividades a impulsar la innovación tecnológica de las empresas.

**Visión:** Impulsamos, junto a empresas, organizaciones y personas, el conocimiento y la innovación tecnológica para ayudar a crecer, y para crear soluciones a los retos del mundo digital, verde y social que imaginamos.

**Objetivos:** Para alcanzar esta visión, los objetivos marcados en la estrategia son:

1. Ser referentes en conocimiento e impulsores de la innovación tecnológica aportando visión y soluciones a los nuevos retos de la sociedad. Y en especial, a las pymes aragonesas, desarrollando el tejido empresarial generando mayor impacto positivo.
2. Ser colaboradores y conectores en el ecosistema público-privado de innovación, aprovechando todas las oportunidades y capacidades en Aragón, España y Europa y el Digital Innovation Hub.
3. Crear nuevos modelos de relación con emprendedores, pymes y empresas, haciendo un esfuerzo por llegar a todo el territorio.
4. Ser ejemplo y motor para la transformación digital, agilidad e innovación en la administración pública, impulsando a la ciudadanía y al sector privado en el proceso.
5. Formar y capacitar tecnológicamente a mujeres y hombres, que estén preparados para una nueva sociedad más digital y sostenible.
6. Reenfocar la estrategia de comunicación, aportando valor y conocimiento, que atraiga talento tecnológico y fomente vocaciones STEAM especialmente entre las niñas y jóvenes.
7. Ser una organización innovadora, digital y abierta, preparada para dar respuestas ágiles frente a cualquier situación en un mundo cada vez más cambiante tecnológicamente.

## 03. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD

La política de seguridad de las tecnologías de la información de ITAINNOVA, en adelante Política de Seguridad TI, persigue la consecución de los siguientes objetivos:

- a. Garantizar a la ciudadanía que los datos alojados en ITAINNOVA serán gestionados de acuerdo a los estándares y buenas prácticas en seguridad TI.
- b. Aumentar el nivel de concienciación en materia de seguridad TI allí donde es de aplicación esta Política, garantizando que el personal a su servicio es consciente de sus obligaciones y responsabilidades.
- c. Establecer las bases de un modelo integral de gestión de la seguridad TI en la Administración de ITAINNOVA, que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales.
- d. Hacer patente el compromiso de ITAINNOVA con la seguridad de la información mediante su apoyo a la Comisión de Seguridad y Protección de Datos, en adelante la Comisión de Seguridad, dotándole de los medios y facultades necesarias para la realización de sus funciones.
- e. Definir, desarrollar y poner en funcionamiento los controles metodológicos técnicos, organizativos y de gestión, necesarios para garantizar de un modo efectivo y medible la preservación de los niveles de confidencialidad, disponibilidad e integridad de la información aprobados por ITAINNOVA.
- f. Garantizar la continuidad de los servicios ofrecidos por ITAINNOVA a la ciudadanía.
- g. Crear y promover de manera continua una “cultura de seguridad” tanto internamente, a todo el personal, como externamente a la ciudadanía y proveedores que permita asegurar la eficiencia y eficacia de los controles implantados y aumente la confianza de nuestra ciudadanía.

## 04. REVISIÓN DE LA POLÍTICA

Esta política será revisada al menos una vez al año y siempre que haya cambios relevantes en la organización, con el fin de asegurar que ésta se adecua a la estrategia y necesidades de la organización.

La Política será propuesta y revisada por el Comité de Seguridad y comunicada al Comité de Empresa con la posibilidad de emitir un informe al respecto de la modificación. Una vez aprobada será difundida por ITAINNOVA para que la conozcan todas las partes afectadas.

En caso de conflictos o diferentes interpretaciones de esta política se recurrirá al Comité de Seguridad para resolución de estos, previo informe propuesta del equipo de Servicios de TI.

## 05. MARCO NORMATIVO

A los efectos previstos en esta Política, el marco normativo de referencia es que estipula la legislación vigente en materia de seguridad TI.

Debido al carácter personal y reservado de la información manejada y a los servicios puestos a disposición de la ciudadanía ITAINNOVA desarrolla sus actividades de acuerdo a la normativa vigente en dichas materias, de entre las que actualmente cabe destacar por su especial relevancia:

- a. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- b. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- c. 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.
- d. 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
- e. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- f. Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- g. 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)
- h. Ley 59/2003, de 19 de diciembre, de firma electrónica.
- i. 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.
- j. Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- k. 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 en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).
- l. Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- m. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- n. Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- o. Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- p. Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

## 06. ÁMBITO DE APLICACIÓN

Esta Política será de aplicación y de obligado cumplimiento para todos los Equipos y Tecnologías de ITAINNOVA, entendiendo por Equipos y Tecnologías a sus diferentes áreas corporativas y tecnológicas; a sus recursos y a los procesos afectados por el ENS y el RGPD, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

## 07. PRINCIPIOS DE SEGURIDAD TI

### 07.1. PRINCIPIOS DE SEGURIDAD TI

La política de seguridad TI de ITAINNOVA se desarrollará, con carácter general, de acuerdo a los siguientes principios:

- a) Principio de confidencialidad: los activos TI deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.
- b) Principio de integridad y calidad: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de esta, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.
- c) Principio de disponibilidad y continuidad: se garantizará un alto nivel de disponibilidad en los activos TI y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.
- d) Principio de trazabilidad: se implantarán medidas para asegurar que en todo momento se pueda determinar quién hizo qué y en qué momento, con el fin de tener capacidad de análisis sobre los incidentes de seguridad detectados.
- e) Principio de autenticidad: se deberá articular medidas para garantizar la fuente de información de la que proceden los datos y que las entidades donde se origina la información son quienes dicen ser.
- f) Principio de gestión del riesgo y de la seguridad integral: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los activos TI.



- 
- g) Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los activos TI deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.
  - h) Principio de concienciación y formación: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información se refiere. De igual forma, se fomentará la formación específica en materia de seguridad TI de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.
  - i) Principio de prevención, reacción y recuperación: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TI.
  - j) Principio de mejora continua o de la reevaluación periódica: se revisará el grado de eficacia de los controles de seguridad TI implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico.
  - k) Principio de seguridad en el ciclo de vida de los activos TI o líneas de defensa: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
  - l) Principio de función diferenciada: la responsabilidad de la seguridad de los sistemas estará diferenciada de la responsabilidad del servicio, así como de la responsabilidad de la información. Los roles y responsabilidades de cada una de estas funciones deberán quedar debidamente acotadas y reflejadas documentalmente.

## 07.2. Requisitos Mínimos de Seguridad

Esta política de seguridad se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

- a) Organización e implantación del proceso de seguridad: La estructura organizativa para la gestión de la seguridad de la información será competente para mantener, actualizar y hacer cumplir, la Política de Seguridad de la Información de ITAINNOVA, así como para garantizar la implantación del proceso de seguridad en la entidad.
- b) Análisis y gestión de los riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el

coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

c) Gestión del personal: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) 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. El personal que atiende, revisa y audita la seguridad de los sistemas recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables. Se exigirá, de manera objetiva y no discriminatoria, que los prestadores de servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

e) Autorización y control de los accesos: Se limitará el acceso a los activos de información por parte de personas usuarias, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

f) Protección de las instalaciones: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

g) Adquisición de productos: En la adquisición de productos de seguridad será exigible la certificación de la funcionalidad de seguridad relacionada con el objeto de dicha adquisición, según el criterio del responsable de seguridad y aplicando el principio de proporcionalidad. Para la contratación de servicios de seguridad se estará a lo dispuesto en el principio de profesionalidad.

h) Seguridad por defecto: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

i) Integridad y actualización del sistema: El sistema informático de ITAINNOVA será diseñado y mantenido por la persona responsable del servicio bajo criterios técnicos, de eficiencia y de seguridad. Todo elemento físico o lógico requerirá autorización formal previa a su

instalación en el sistema. También requerirá autorización formal previa cualquier alteración de la configuración de hardware y software de los equipos o cualquier desinstalación de programas de la plataforma de uso predefinida. Con carácter general, no se instalará software salvo que se disponga de la correspondiente licencia de uso, bien por haberlo adquirido ITAINNOVA, o bien por tratarse de software libre con una licencia aplicable. En todo caso, será el/la administrador/a del sistema quien instale el software una vez se autorice

j) Protección de la información almacenada y en tránsito: En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros, como los equipos portátiles (PCs, móviles o tabletas), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil. También forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por ITAINNOVA.

k) Prevención ante otros sistemas de información interconectados: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

l) Registro de actividad: Se registrarán las actividades de las personas usuarias, 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.

m) Incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad

n) Continuidad de la actividad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus personas usuarias.

o) Mejora continua del proceso de seguridad: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

## 08. Organización de la seguridad TI

## 08.1. Responsabilidad general

La preservación de la seguridad TI será considerada objetivo común de todas las personas al servicio de ITAINNOVA, siendo estas responsables del uso correcto de los activos de tecnologías de la información y comunicaciones puestos a su disposición.

En caso de incumplimiento de las directrices y normativas de seguridad indicadas en la presente política y las obligaciones derivadas de ellas, ITAINNOVA se reserva el derecho de aplicar el régimen disciplinario establecido en el Estatuto Básico del Empleado Público aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre y en las normas que las Leyes de Función Pública dicten en desarrollo del mismo.

Por su importancia dentro de la implementación de la seguridad, quedan desarrolladas en la presente política algunas de las funciones de los órganos que ITAINNOVA estima necesarios para la correcta gestión de la seguridad.

La estructura organizativa de ITAINNOVA en materia de Seguridad se revisa al comienzo de cada legislatura. Una vez revisada, ITAINNOVA celebra un Comité de Seguridad Extraordinario donde se ratifica la nueva organización de la seguridad (Presidente, vocales, secretario, responsable de seguridad, ...).

## 08.2. Comisión de Seguridad

1. Se crea el Comisión de Seguridad de ITAINNOVA, como órgano colegiado de carácter transversal para la coordinación y gobierno en materia de seguridad en el ámbito de la entidad.
2. La Comisión estará formada por los siguientes representantes de ITAINNOVA: dirección, gerencia, y responsable del Equipo de Servicios de TI.
3. Serán funciones propias de la Comisión:
  - a) Definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos en seguridad TI.
  - b) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos.
  - c) Elevación de propuestas de revisión del marco normativo de seguridad TI al órgano competente para su reglamentaria tramitación.
  - d) Establecimiento de directrices comunes y supervisión del cumplimiento de la normativa en materia de seguridad TI.
  - e) Supervisión y aprobación del nivel de riesgo y de la toma de decisiones en la respuesta a incidentes de seguridad que afecten a los activos TI.
  - f) Definición y aprobación del modelo de relación con los Comisión de Seguridad TI de las entidades incluidas en el ámbito de aplicación de la Política.
4. La Comisión de Seguridad se reunirá al menos una vez por semestre y se regirá por esta política.
5. La Comisión de Seguridad nombrará entre sus miembros un grupo de respuesta a incidentes TI, llamado "Comité de Crisis", cuya función será la

toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de sistemas de información críticos de ITAINNOVA.

6. Las labores de soporte y asesoramiento a la Comisión de Seguridad serán realizadas por la persona Responsable de Seguridad y la Oficina de Seguridad y Protección de Datos.

### **08.3. Responsable de seguridad TI**

1. El nombramiento de la persona Responsable de Seguridad será potestad de la Comisión de Seguridad.

2. La persona Responsable de Seguridad tendrá las siguientes funciones, dentro de su ámbito:

- a) Definición y seguimiento de las actuaciones relacionadas con la seguridad TI de los activos de información de la entidad y la gestión del riesgo.

- b) Asesoramiento y soporte sobre temas de Seguridad.

- c) Coordinación en materias de seguridad TI.

- d) Propuesta y seguimiento de programas de formación y concienciación.

- e) Reporte a la Comisión de Seguridad de un informe periódico sobre el estado de la Seguridad TI y las actividades relacionadas.

- g) Asunción de las funciones incluidas en los artículos 10, 27.3, 34.6, Anexo II (apartado 2.3) y Anexo III (apartados 2.1.b y 2.2.b) 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.

- f) Asunción de las funciones incluidas en el Reglamento UE2016-679 que regula la Protección de Datos de Carácter Personal, aprobado el 25 de mayo de 2016 y que entró en vigor el 25 de mayo de 2017.

### **08.4. Oficina de Seguridad TI**

La Oficina de Seguridad TI estará compuesto por las personas Responsables de Equipo y Agrupaciones Tecnológicas de ITAINNOVA, si bien se puede convocar a aquellas personas que la Oficina estime necesarias para el desarrollo de los trabajos encomendados.

En esta Oficina de Seguridad TI estará también la persona Responsable de Seguridad de ITAINNOVA que tendrá funciones sobre la revisión y elaboración de propuestas para ser presentadas y debatidas en el Comité de Seguridad TI.

- 
1. La Oficina de Seguridad y Protección de Datos tendrá las siguientes atribuciones:
    - a) Definición del planteamiento técnico y operativo de los objetivos, iniciativas y planes estratégicos en seguridad TI, de acuerdo con las directrices del Comité de Seguridad TI.
    - b) Elaboración de propuestas relativas a la revisión del marco normativo de seguridad TI.
    - c) Elaboración de informes y propuestas de cumplimiento legal y normativo.
    - d) Elaboración de informes sobre el nivel de seguridad TI de los activos.
    - e) Reporte al Comité Seguridad TI de informes periódicos sobre el estado de la Seguridad TI de ITAINNOVA.
  2. La Oficina de Seguridad y Protección de Datos se regirá por esta Política.

## 08.5. Responsables

La persona Responsable de la Información determina los requisitos de seguridad respecto a la información tratada en ITAINNOVA.

La persona Responsable del Servicio determina la infraestructura hardware y software del sistema de información, los criterios de uso, los servicios ofrecidos, los formatos y cualquier otro aspecto del funcionamiento del sistema de información de ITAINNOVA.

La persona Responsable de Seguridad determina cómo satisfacer los requisitos de seguridad, tanto de la información como de los servicios ofrecidos, incluyendo la definición de procedimientos de seguridad y, en su caso, la adopción de medidas de urgencia ante posibles deficiencias o amenazas en ITAINNOVA.

El/la administrador/a del sistema desarrolla, opera y mantiene el sistema de información de ITAINNOVA.

Las discrepancias en materia de seguridad serán resueltas atendiendo al criterio de mayor jerarquía.

Las atribuciones de cada responsable, así como los mecanismos de coordinación y resolución de conflictos se explicitan en la Normativa de Roles y Responsabilidades de Seguridad y la Normativa de la Organización de la Seguridad.

## 09. Desarrollo de la Política de Seguridad

### 09.1. Instrumentos del desarrollo

La Política de Seguridad de la Información de ITAINNOVA se desarrollará por medio de instrucciones de servicio y circulares que afronten aspectos específicos. Dichas instrucciones y circulares podrán adoptar alguna de las siguientes modalidades:

Se usarán los siguientes instrumentos:

**Normas de seguridad:** Uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de las personas usuarias. Son de carácter obligatorio.

**Procedimientos:** Concretan flujos de trabajo para la realización de tareas, indicando lo que hay que hacer, paso a paso, pero sin entrar en detalles (de proveedores, marcas comerciales o comandos técnicos). Son útiles en tareas repetitivas.

**Instrucciones técnicas:** Desarrollan los Procedimientos llegando al máximo nivel de detalle, (indicando proveedores, marcas comerciales y comandos técnicos empleados para la realización de las tareas).

La normativa de seguridad estará disponible en el Portal Interno de la entidad a disposición de todos los miembros de la organización que necesiten conocerla. De igual forma se informará de la misma a las nuevas incorporaciones mediante su incorporación al proceso de acogida. Así mismo, cada vez que haya un cambio a este documento de forma consensuada se publicará la nueva versión y se comunicará a toda la organización.

### 09.2. Aprobación de las normativas

En toda la organización, la aprobación de las normas de seguridad se hará de acuerdo con lo dispuesto en la presente política y las normativas específicas que para ello desarrollará ITAINNOVA.

### 09.3. Sanciones previstas por incumplimiento

Del incumplimiento de la Política de Seguridad de la Información y normas que la desarrollan podrán derivarse las consiguientes responsabilidades disciplinarias, que se sustanciarán conforme a lo establecido en la normativa sobre régimen disciplinario de las personas vinculadas a ITAINNOVA, así como, en su caso, a lo prevenido en el Convenio Colectivo vigente en cada momento.

## 10. Concienciación y Formación

Con la concienciación y formación se busca alcanzar varios objetivos. Por una parte y fundamental la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de ITAINNOVA y a todas las actividades y servicios que lo componen.

Por otra parte, y siguiendo el Principio de Seguridad Integral, la articulación de los medios necesarios para que todas las personas que intervienen en el día a día de ITAINNOVA y sus responsables jerárquicos tengan la sensibilidad adecuada hacia la responsabilidad que conlleva al gestionar información de la ciudadanía y de la propia Administración.

## 11. Análisis y Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- Al menos una vez al año (mediante revisión y aprobación formal).
- Cuando ocurra un incidente grave de seguridad.

Para el análisis y gestión de riesgos se usará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), elaborada por el Consejo Superior de Administración Electrónica y enfocada a las Administraciones Públicas.

## 12. Seguridad de la información

Se desarrollará una Clasificación de la Información de ITAINNOVA de forma que se identifiquen los distintos tipos de información, en base a su sensibilidad, se establezca cómo etiquetar los soportes que la contengan y se determine qué se puede y no se debe hacer con cada nivel de clasificación.



---

## 13. Datos de Carácter Personal

Será de aplicación lo contemplado en el RGPD y lo dispuesto en la legislación nacional a tales efectos.

Cada departamento se encargará de gestionar y mantener la seguridad referente a los datos de carácter personal incluidos en las operaciones de tratamiento que a tal efecto sean de su responsabilidad.

Todos los sistemas de información de ITAINNOVA se ajustarán a los niveles de seguridad requeridos por esta normativa.

## 14. Obligaciones del personal

Todos los miembros de la organización y las empresas y personas terceras que realicen servicios de cualquier clase contratados por ITAINNOVA o que de alguna manera se presten bajo el control y/o la dirección de ITAINNOVA tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, que será trasladada a través de los correspondientes Equipos y Agrupaciones Tecnológicas quienes deberán disponer los medios necesarios para que ésta llegue a los afectados.

Se establecerá un programa de concienciación continua dirigido a todos los miembros de ITAINNOVA, en particular a los de nueva incorporación.

El personal deberá usar los procedimientos de notificación de incidentes de seguridad habilitados a tal efecto, en caso de detectar un posible incidente.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas.

## 15. Terceras partes

Cuando ITAINNOVA preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para el reporte y coordinación de los respectivos con la Comisión de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando ITAINNOVA utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información. Dicha tercera parte deberá aceptar el quedar sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios

procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, 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 requerirá un informe del Responsable de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados, así como del responsable del tratamiento previsto en el RGPD, antes de seguir adelante.

## 16. ANEXO I

### Glosario de términos

**Política de seguridad de la información:** Conjunto de directrices plasmadas en un documento escrito, que rigen la forma en que una organización gestiona y protege sus activos de tecnologías de la información.

**Activo de tecnologías de la información:** cualquier información o sistema de información que tenga valor para la organización. Incluye datos, servicios, aplicaciones, equipos, comunicaciones, instalaciones, procesos y recursos humanos.

**Incidente de seguridad TI:** Suceso, accidental o intencionado, a consecuencia del cual se ve afectada la integridad, confidencialidad o disponibilidad de la información.

**Contingencia grave:** Incidente de seguridad TI cuya ocurrencia causaría la reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, el sufrimiento de un daño significativo a los activos de la organización, el incumplimiento material de alguna ley o regulación, o un perjuicio significativo de difícil reparación a personas.

**Plan director de seguridad:** Estrategia y conjunto de iniciativas planificadas, plasmadas en un documento escrito, cuyo objetivo es alcanzar un determinado nivel de seguridad en la organización.

**Riesgo:** Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

**Sistema de información:** Conjunto organizado de recursos destinado a recoger, almacenar, procesar, presentar o transmitir la información.

**Sistema de información crítico:** Sistema de información cuyo adecuado funcionamiento es indispensable para el funcionamiento de la organización y el cumplimiento de sus obligaciones fundamentales.

## 17. CONTROL DE CAMBIOS

Versión	Fecha	Autor	Descripción
Inicial		Cibergob	Creación del documento
1	03/03/2022	Comité de Seguridad	Aprobado el documento
1.1	12/06/2023	Comité de Seguridad	Revisión tras apertura de trámite de consulta a comité de empresa
1.2	20/10/2023	Comité de Seguridad	Revisión tras trámite de consulta a comité de empresa.