# ÍNDICE

# 1. OBJETIVO

La presente Política de Seguridad de la Información constituye el marco de referencia que rige la forma en que Pragmatech AI Solutions gestiona y protege la información que trata y los servicios que presta, incluidos los prestados a entidades del sector público. Su aprobación da cumplimiento al artículo 2.3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que extiende su aplicación a los sistemas de información de las entidades del sector privado cuando presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas. En base a esta norma y legislación se han determinado en el conjunto de documentos que conforman el marco de seguridad de la información de la organización.

La presente Política de Seguridad es una línea de actuación clara, manifiesta y pública de Pragmatech AI Solutions, por lo que la Dirección expresa su apoyo total a la misma y se compromete a mantener las directrices fijadas en el presente Documento.

La presente Política de la Seguridad de la Información y tendrá vigencia una vez aprobada por la Dirección, poniéndose en conocimiento de todo el personal de la organización, incluidos aquellos externos a los que sea de aplicación. La presente política está alineada con las directrices de las leyes y regulaciones existentes y proporciona un marco de referencia para el establecimiento de los objetivos de seguridad de la información. Cualquier conflicto con estas regulaciones debe ser informado inmediatamente a la organización.

Toda violación de la presente política o de las normas y procedimientos que las desarrollan, será considerado por el procedimiento disciplinario, incluyéndose proveedores y colaboradores externos.

En virtud de lo expuesto, la Política de Seguridad de la Información de Pragmatech AI Solutions se regirá por lo dispuesto en los siguientes apartados.

# 2. ALCANCE

Esta política se aplica a los sistemas de información de Pragmatech AI Solutions que dan soporte a los servicios de diseño y desarrollo, soporte y mantenimiento del software sanitario destinado a hospitales, centros de atención primaria y/o centros médicos clientes, según el alcance definido en el documento de Categorización del sistema.

Cuando la prestación del servicio se realiza sobre infraestructura ajena a la organización, la explotación y operación en dicho entorno son responsabilidad del cliente y quedan fuera del alcance de esta política,

sin perjuicio de las obligaciones que Pragmatech AI Solutions asume como fabricante del producto sanitario y, en su caso, como encargada del tratamiento.

El alcance comprende la información en cualquier soporte y ubicación, incluyendo las instalaciones de trabajo de la organización, los servicios en la nube contratados, los entornos de diseño y desarrollo, y los puestos de trabajo en movilidad o teletrabajo.

La política es de obligado cumplimiento para todo el personal de Pragmatech AI Solutions, con independencia de su relación laboral, así como para los socios, subcontratistas y colaboradores externos que participen en la prestación de los servicios comprendidos en el alcance.

Los criterios que determinan el nivel de seguridad requerido, atendiendo a la categorización del sistema y a la valoración de los servicios soportados y de la información manejada por éstos, están definidos en el documento de Categorización del sistema. Considerando lo establecido en dicho documento, la valoración general del sistema de Pragmatech AI Solutions es categoría ALTA, tomando como referencia la guía CCN-STIC-803 de Valoración de los Sistemas.

# 3. MISIÓN Y OBJETIVOS DE SEGURIDAD

Pragmatech AI Solutions es una empresa tecnológica especializada en el desarrollo de soluciones de software sanitario basadas en inteligencia artificial, especializada en el desarrollo de software sanitario basado en inteligencia artificial. Su producto cuenta con marcado CE conforme al Reglamento (UE) 2017/745 de productos sanitarios y la compañía opera bajo un sistema de gestión de la calidad alineado con las normas ISO 13485 e IEC 62304.

En el ejercicio de esta actividad, Pragmatech AI Solutions trata, en las labores de soporte y validación del producto, datos de carácter personal relativos a la salud (categoría especial del artículo 9 del RGPD). La empresa actúa como encargada del tratamiento respecto de los datos personales cuya responsabilidad ostentan los centros sanitarios clientes, lo que obliga a cumplir simultáneamente las exigencias del ENS y del Reglamento General de Protección de Datos.

Para proteger estos activos y garantizar la continuidad de los servicios comprometidos, así como para mantener la reputación e imagen de la entidad, Pragmatech AI Solutions se compromete a preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y de los servicios.

Pragmatech AI Solutions, S.L. establece como **objetivos de seguridad** de la información los siguientes:

- Preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y de los servicios en el alcance.
- Cumplir el marco legal y regulatorio aplicable: el ENS (RD 311/2022), la normativa de protección de datos (RGPD y LOPDGDD), atendiendo al carácter especial de los datos de salud, y la regulación de producto sanitario (MDR), tanto en la condición de responsable como de encargado del tratamiento.
- Gestionar los riesgos de seguridad de forma continua, manteniendo el riesgo residual en niveles aceptables conforme al análisis de riesgos.
- Asegurar la continuidad de los servicios de desarrollo, soporte y mantenimiento, conforme a los objetivos de recuperación (RTO/RPO) establecidos.
- Gestionar los incidentes de seguridad de manera eficaz, garantizando su detección, respuesta y notificación a las autoridades competentes cuando proceda.
- Promover la formación y concienciación de todo el personal en materia de seguridad de la información.
- Mejorar de forma continua el sistema de gestión de la seguridad.

El grado de consecución de estos objetivos se mide a través del Cuadro de Indicadores.

La Dirección, comprometida con la implantación y el mantenimiento del proceso integral de seguridad de la información, fijará y aprobará periódicamente unos objetivos de nivel de riesgo aceptable en el Comité de Seguridad de la Información. Dichos objetivos estarán alineados con el propósito y la estrategia de la organización, serán medibles o estimables y coherentes con las presentes directrices.

# 4. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información aplica los principios básicos que se establecen en el ENS, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permitiendo una protección adecuada de la información y los servicios.

Atendiendo al ENS, Pragmatech AI Solutions implementa diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger, teniendo en cuenta la categoría de los sistemas afectados, bajo los siguientes principios:

## 4.1 La seguridad como proceso integral

La seguridad de la información en Pragmatech AI Solutions debe contar con el compromiso y apoyo de la Dirección de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz. La seguridad constituye un proceso integral compuesto por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema basado en la mejora continua de todos ellos y del proceso en sí mismo.

Se debe prestar la máxima atención a la formación y concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.

## 4.2 Prevención, detección, respuesta y conservación

Pragmatech AI Solutions implementa un proceso integral de prevención, detección, respuesta y conservación frente a incidentes de seguridad con procedimientos de detección, análisis, comunicación, resolución y registro de las actuaciones para la mejora continua de la seguridad de los sistemas, designando un punto de contacto para las comunicaciones con respecto a incidentes detectados y estableciendo protocolos para el intercambio de información relacionada con el incidente, incluyendo las comunicaciones con los Equipos de Respuesta a Emergencias (CERT).

## 4.3 Líneas de defensa

Pragmatech AI Solutions implementa una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falla, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse;
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto y
- Minimizar el impacto final sobre el mismo.

## 4.4 Vigilancia continua

La vigilancia continua exige la monitorización de los registros de actividad. Se registrará la información estrictamente necesaria para la investigación de actividades indebidas o no autorizadas que permitan identificar al responsable de la actividad.

### 4.5 Reevaluación periódica

Pragmatech AI Solutions implementa controles y evaluaciones regulares y periódicas de la seguridad, de forma interna o con la ayuda de terceros, para conocer en todo momento el estado de la seguridad de los sistemas y adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

### 4.6 Diferenciación de responsabilidades

Se organiza la seguridad comprometiendo a todos los miembros de Pragmatech AI Solutions mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas.
Se nombrarán, al menos, el responsable de la información, el responsable del servicio, el responsable de seguridad, y el responsable del sistema, quedando diferenciada la responsabilidad de la seguridad de la responsabilidad de explotación de los sistemas.

## 5. MARCO NORMATIVO

La presente política se desarrolla conforme al marco legal vigente en materia de seguridad de la información, incluyendo el Esquema Nacional de Seguridad (Real Decreto 311/2022 de 3 de mayo), en adelante ENS, el Reglamento General de Protección de Datos (RGPD) y demás normativas aplicables recogidas en la documentación de seguridad de la organización.

## 6. COMITÉ DE SEGURIDAD

La Seguridad de la Información será regida por un Comité de Seguridad. Dicho comité estará formado por los siguientes perfiles:

- Dirección como Responsable del Sistema en el ámbito del ENS.
- Responsable del Sistema de Gestión de Calidad como Responsable de Seguridad.
- Dirección Comercial como Responsable de la Información y Responsable del Servicio.

Integran asimismo el Comité el Administrador de Seguridad y, como invitado, con voz pero sin voto, el Delegado de Protección de Datos (externo), que será convocado cuando los asuntos tratados afecten a la protección de datos personales. Además de los miembros permanentes, podrá requerirse la participación en el Comité de Seguridad de otros responsables o personal de la organización, así como de socios,

colaboradores, profesionales externos u otros terceros, cuando los asuntos tratados así lo requieran, previa convocatoria (sujetos al deber de confidencialidad y actuando con voz, pero sin voto).

Las funciones del Comité de Seguridad, las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos se detallan en el Procedimiento de Designación de Roles y Segregación de Funciones y en el Acta de Constitución del Comité de Seguridad.

# 7. ROLES

Además de las funciones comunes definidas para el Comité de Seguridad, se han definido una serie de roles y sus responsabilidades en el Procedimiento de Designación de Roles y Segregación de Funciones.

La designación y nombramiento de roles será llevada a cabo por la Dirección de Pragmatech AI Solutions, S.L., quien podrá recabar el asesoramiento del Comité de Seguridad o de cualquier personal de la organización. Se renovarán de forma automática con carácter anual salvo que desde dirección se estime oportuno un cambio en estas designaciones.

# 8. PERSONA DE CONTACTO (POC)

El Responsable de Seguridad actuará como PoC (Persona de Contacto) inicial para la seguridad de la información tratada y el servicio prestado a los clientes, de conformidad con lo descrito en el Procedimiento de Designación de Roles y Segregación de Funciones.

# 9. RESOLUCIÓN DE CONFLICTOS

Los conflictos que pudieran surgir entre los distintos responsables en el ejercicio de sus funciones serán resueltos por el Comité de Seguridad de la Información, conforme a los mecanismos de coordinación y resolución de conflictos previstos en el Procedimiento de Designación de Roles y Segregación de Funciones.

# 10. REQUISITOS MÍNIMOS

Pragmatech AI Solutions, S.L. depende de los sistemas de Tecnologías de la Información y las Comunicaciones (en adelante, TIC) para alcanzar sus objetivos. Estos sistemas deben administrarse con diligencia, adoptando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados

que puedan afectar a la disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad de la información tratada o de los servicios prestados.

Los sistemas TIC deben estar protegidos frente a amenazas de rápida evolución con potencial para incidir en cualquiera de las cinco dimensiones de la seguridad. Para defenderse de ellas se requiere una estrategia capaz de adaptarse a los cambios del entorno y garantizar la prestación continua de los servicios. Como entidad del sector privado que presta servicios a entidades del sector público y que, por ello, queda dentro del ámbito de aplicación del Esquema Nacional de Seguridad, Pragmatech AI Solutions, S.L. dispone formalmente de la presente Política de Seguridad de la Información, aprobada por la Dirección de la organización.

En consecuencia, Pragmatech AI Solutions, S.L. aplicará las medidas mínimas de seguridad exigidas por el ENS, realizará un seguimiento continuo de los niveles de prestación de los servicios, seguirá y analizará las vulnerabilidades reportadas y preparará una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Todas las áreas velarán por que la seguridad TIC sea parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada del servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación se identificarán e incluirán en la planificación y, en su caso, en los procesos de contratación. La organización estará preparada para prevenir, detectar, reaccionar y recuperarse de incidentes.

## 10.1 Datos de carácter personal

Pragmatech AI Solutions, S.L. solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades para los que se hayan obtenido, cumpliendo las obligaciones y principios recogidos en la normativa de protección de datos vigente en cada momento.

Asimismo, adoptará las medidas de índole técnica y organizativa necesarias para el cumplimiento de dicha normativa, conforme a lo establecido en la normativa interna de la organización relativa a la protección de datos de carácter personal.

## 10.2 Análisis y gestión de los riesgos

Pragmatech AI Solutions, S.L. asume el compromiso de controlar los riesgos de seguridad y de dar cumplimiento a la legislación y a las normas internas vigentes, bajo un proceso de mejora continua conforme a los marcos y metodologías de análisis y gestión de riesgos reconocidos en la actualidad.

Con el objetivo de conocer el nivel de exposición de los activos de información a los riesgos y amenazas de seguridad, el Responsable de Seguridad acordará la realización de un análisis de riesgos cuyas conclusiones se plasmarán en actuaciones para tratar y mitigar el riesgo. Dichas actuaciones deberán estar justificadas y ser proporcionales al riesgo a mitigar, pudiendo incluso replantear la seguridad de los sistemas en caso necesario.

Se contemplará la realización adicional de un análisis de riesgos de los sistemas de información cuando:

- Se modifique de manera importante la infraestructura del sistema de información.
- Se modifiquen los servicios prestados.
- Ocurran incidentes graves de seguridad.
- Se reporten vulnerabilidades graves que afecten a los sistemas de información de la organización.

Las conclusiones de los análisis de riesgos serán revisadas por el Responsable de Seguridad, que las comunicará al Comité de Seguridad de la Información.

### 10.2.1 Criterios de evaluación de riesgos

Para la armonización de los análisis de riesgos, Pragmatech AI Solutions, S.L. ha establecido una valoración de referencia para los distintos tipos de información manejados y los diferentes servicios prestados. Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos desarrollada internamente.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir de forma grave la prestación de los servicios o el cumplimiento de la misión de la organización. Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de los servicios.

### 10.2.2 Directrices de tratamiento de riesgos

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

### 10.2.3 Proceso de aceptación del riesgo residual

Los riesgos residuales serán determinados por el Responsable de Seguridad.

Los niveles de riesgo residual esperados sobre cada información, tras la implementación de las opciones de tratamiento previstas, deberán ser aceptados previamente por el responsable de esa información.

Los niveles de riesgo residual esperados sobre cada servicio, tras la implementación de las opciones de tratamiento previstas, deberán ser aceptados previamente por el responsable de ese servicio.

Los niveles de riesgo residual serán presentados por el Responsable de Seguridad al Comité de Seguridad de la Información, para que este proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

## 10.3 Gestión de incidentes de seguridad

### 10.3.1 Monitorización y detección de incidentes

En Pragmatech AI Solutions, S.L. existen sistemas de monitorización para la detección, el análisis y el reporte de incidentes. Estos se recogen en el procedimiento interno de control de los sistemas en operación.

### 10.3.2 Respuesta ante incidentes

Para garantizar la disponibilidad de los servicios y la protección de la información, Pragmatech AI Solutions, S.L. dispone de un procedimiento de gestión de incidentes. Asimismo, dispone de un plan de contingencia.

Los planes de continuidad de los sistemas TIC se desarrollan por el Responsable del Sistema.

Se dispone de procedimientos específicos, actualizados periódicamente, de reporte y resolución de incidencias.

## 10.4 Gestión del personal

### 10.4.1 Obligaciones del personal

Todo el personal de Pragmatech AI Solutions, S.L. tiene la obligación de conocer y cumplir la presente Política de Seguridad, así como las normativas y los procedimientos derivados de la misma, entre los que se encuentran los relativos a la protección de datos de carácter personal. El Responsable de Seguridad dispondrá de los mecanismos necesarios para que esta información llegue a todo el personal.

El incumplimiento manifiesto de la Política de Seguridad de la Información, o de la normativa y procedimientos derivados de esta, podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, la exigencia de las responsabilidades legales correspondientes, conforme al régimen disciplinario establecido en la normativa interna de Pragmatech AI Solutions, S.L. y en la legislación laboral vigente.

### 10.4.2 Terceras partes

Cuando se presten servicios o se gestione información de algún usuario o entidad externa, se les hará partícipes de la Política de Seguridad de la Información y se establecerán canales para el reporte y la coordinación en materia de seguridad.

Cuando se presente información a usuarios externos, se les hará partícipes de la presente Política en lo que ataña a dichos servicios o información. La tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en este documento.

Cuando algún aspecto recogido en el presente documento no pueda ser satisfecho por una tercera parte conforme a lo indicado en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Dicho informe deberá ser aprobado por los responsables de la información y de los servicios afectados antes de continuar.

### 10.4.3 Concienciación y formación

Los miembros de la organización asistirán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año, y se establecerá un programa de concienciación continua dirigido al personal de la organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de los sistemas TIC recibirán la formación necesaria para el manejo seguro de los sistemas, en la medida en que la precisen para el desempeño de su trabajo. La formación será obligatoria antes de asumir una responsabilidad, ya sea su primera asignación o un cambio de puesto de trabajo o de responsabilidades en el mismo.

### 10.4.4 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.

Asimismo, se procurará que, de manera objetiva y no discriminatoria, las organizaciones que presten servicios de seguridad a Pragmatech AI Solutions, S.L. cuenten con niveles idóneos de gestión y madurez en los servicios prestados.

## 10.5 Autorización y control de los accesos

El acceso a los sistemas de información deberá estar controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información debidamente autorizados, restringiendo el acceso a las funciones permitidas. Dicha responsabilidad recaerá sobre el Responsable de Seguridad.

Los responsables internos deberán velar, en el ámbito de sus servicios y competencias, por el cumplimiento de las instrucciones de coordinación, medidas y estrategias que determine el Responsable de Seguridad.

Para poder corregir o exigir responsabilidades, cada usuario que acceda a la información del sistema deberá identificarse de forma única, de modo que se conozca, en todo momento, quién recibe derechos de acceso, de qué tipo son y quién ha realizado una determinada actividad.

## 10.6 Protección de las instalaciones

Los sistemas de información y los soportes que contienen información sensible se ubicarán en áreas protegidas, dotadas de un control de acceso físico adecuado a la categoría del sistema, de forma que se prevengan accesos no autorizados y se garantice el funcionamiento del resto de medidas de seguridad.

Cuando la actividad se desarrolle en instalaciones cuya gestión corresponda a un tercero, Pragmatech AI Solutions, S.L. identificará las medidas de seguridad física aportadas por el operador de dichas instalaciones y establecerá los controles compensatorios necesarios para garantizar la protección de la información, reduciendo el perímetro de seguridad al propio equipamiento de la organización.

El acceso a las áreas de trabajo, la identificación de las personas, la protección frente a amenazas del entorno y demás medidas de seguridad física se desarrollan en la normativa de seguridad física de la organización.

Los responsables internos velarán, en el ámbito de sus competencias, por el cumplimiento de las instrucciones, medidas y estrategias que determine el Responsable de Seguridad.

## 10.7 Adquisición de productos de seguridad

En la adquisición de productos de seguridad de las TIC, así como de seguridad física, que vayan a ser utilizados por Pragmatech AI Solutions, S.L., se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, y se velará por que así se contemple en las condiciones contractuales.

La certificación indicada deberá ajustarse a las normas y estándares de mayor reconocimiento internacional en el ámbito de la seguridad funcional.

Todos los productos de software y hardware destinados a la seguridad deberán cumplir los requisitos mínimos definidos por el ENS. Estos productos deberán estar certificados conforme a estándares reconocidos por el Centro Criptológico Nacional —a través de la guía CCN-STIC-105— o por otras normativas de seguridad internacionalmente aceptadas.

Los componentes críticos deberán estar certificados, y se verificará el cumplimiento de medidas organizativas y técnicas —como el cifrado, el control de accesos y la protección frente a código dañino— antes de su implementación.

## 10.8 Seguridad por defecto

Los sistemas se diseñarán y configurarán de forma que garanticen la seguridad por defecto:

- El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos, y ninguna otra funcionalidad adicional.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que solo sean accesibles por las personas, o desde los emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y de puntos de acceso.
- En un sistema en explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin perseguido.
- El uso ordinario del sistema deberá ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

## 10.9 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 con las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista de dicho estado de seguridad.

## 10.10 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. Tendrán la consideración de entornos inseguros, entre otros, los siguientes dispositivos: equipos portátiles, dispositivos periféricos, soportes de información (memorias USB, discos duros) y comunicaciones sobre redes abiertas o con cifrado débil.

Forman parte de la seguridad los procedimientos que aseguren la recuperación y la conservación a largo plazo de los documentos electrónicos producidos por Pragmatech AI Solutions, S.L. en el ámbito de sus competencias.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de información electrónica deberá estar protegida con el mismo grado de seguridad que esta. A tal efecto se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentre, de conformidad con las normas aplicables a su seguridad.

### 10.11 Prevención ante otros sistemas de información interconectados

El sistema protegerá su perímetro, en particular si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público. En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas, o a través de redes, y se controlará su punto de unión.

### 10.12 Registro de actividad

Con la finalidad exclusiva de lograr el cumplimiento del objeto de la normativa aplicable, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral y demás disposiciones aplicables, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, y permitiendo identificar en cada momento a la persona que actúa.

### 10.13 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.

### 10.14 Mejora continua del proceso de seguridad

El proceso integral de seguridad implantado deberá actualizarse y mejorarse de forma continua. A tal efecto, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de las tecnologías de la información.

## 11. ESTRUCTURACIÓN DE LA DOCUMENTACIÓN

La normativa de seguridad de Pragmatech AI Solutions, S.L. se estructura en cinco niveles:

1. **Políticas:** documento que recoge las intenciones y la dirección de la organización, tal como las expresa formalmente la alta dirección.
2. **Procesos:** documento que relaciona esquemáticamente un conjunto de actividades que utilizan las entradas para proporcionar un resultado previsto.
3. **Procedimientos:** documento en el que se especifica quién, qué, dónde, cuándo y por qué se lleva a cabo un proceso o actividad. El cómo, según el caso, podrá especificarse en el propio procedimiento o en una instrucción de trabajo. Un procedimiento puede describir todo o parte de un proceso de la organización.
4. **Instrucciones de trabajo:** documento en el que se especifica cómo se lleva a cabo un proceso o una actividad concreta.
5. **Formatos, registros y otros:** documentos que contienen la forma y el medio establecidos por la organización para registrar determinadas actividades o procesos, que presentan resultados obtenidos o proporcionan evidencias de actividades realizadas, o que ofrecen información de soporte.

La descripción completa de la estructuración de la documentación se encuentra en el documento interno establecido a tal efecto.

### 11.1 Calificación de la información

La información se califica y trata según su nivel de seguridad. La organización establece cuatro niveles de clasificación, de modo que cada activo de información recibe el tratamiento y las medidas de protección correspondientes a su nivel. Los criterios de clasificación, las responsabilidades y las medidas asociadas se detallan en la Normativa de Clasificación y Conservación de la Información.

## 12. CERTIFICACIÓN DE CONFORMIDAD CON EL ENS

Pragmatech AI Solutions se someterá a la auditoría bienal prevista en el artículo 31 del RD 311/2022 y obtendrá la Certificación de Conformidad con el ENS conforme a los procedimientos de la guía CCN-STIC 809. **La organización** asegurará el nivel de madurez exigido a la Categoría ALTA. Para ello, Pragmatech AI Solutions garantizará que la implantación y eficacia de las medidas de seguridad sean evaluadas de forma sistemática a través de métricas e indicadores objetivos. La certificación se mantendrá vigente, el

distintivo de conformidad se publicará en la sede corporativa y se comunicará a las entidades contratantes. Anualmente se cumplimentará el Informe del Estado de la Seguridad mediante la herramienta INES del CCN, conforme al artículo 32, cuando proceda.

## 13. VIGENCIA Y REVISIÓN

La presente política entrará en vigor al día siguiente de su aprobación por la Dirección de Pragmatech AI Solutions y tendrá vigencia indefinida. Será objeto de revisión al menos anual, así como ante cambios significativos en el marco normativo, en la cartera de servicios, en los sistemas de información, en los resultados del análisis de riesgos, en las conclusiones de las auditorías de certificación o ante incidentes de seguridad relevantes.

## 14. DOCUMENTACIÓN RELACIONADA

La presente Política de Seguridad es el documento de máximo nivel del **marco normativo de seguridad de la información** de Pragmatech AI Solutions, conforme al Esquema Nacional de Seguridad. Todas las directrices aquí establecidas se desarrollan de forma exhaustiva a través de normativas específicas, procedimientos operativos, instrucciones técnicas y registros de evidencia.

Esta documentación interna, de carácter confidencial y de obligado cumplimiento para el personal autorizado, se encuentra estructurada, controlada y centralizada en los repositorios corporativos designados por la organización, garantizando su integridad, actualización continua y disponibilidad para su ejecución y para los correspondientes procesos de auditoría.

## 15. CONTROL DE VERSIONES

La versión en vigor de este documento es, en todo momento, la publicada en el repositorio documental de la empresa. Las copias impresas o almacenadas fuera de dicho repositorio se consideran copias no controladas y su vigencia no está garantizada.

| Versión | Fecha | Descripción del cambio |
|---|---|---|
| 00 | 14/07/2026 | Versión inicial |