Contenido

1. Aprobación y entrada en vigor

Texto aprobado el día 21/10/2025 por la Dirección de PINVESTIGA**.**

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hora hasta que sea reemplazada por una nueva versión.

2. Introducción

PINVESTIGA depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada a los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuidad de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implican que deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de los servicios, seguir y analizar las vulnerabilidad reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

PINVESTIGA debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos TIC.

PINVESTIGA debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

3. Alcance

Sistema de información que da soporte a los servicios de:

- Diseño, desarrollo e implementación de aplicaciones software destinadas para la gestión de información sanitaria.
- Asesoría y gestión de actividades relacionadas con la investigación sanitaria en ensayos clínicos fase III, fase IV y post-autorización de medicamentos y productos sanitarios.

4. Misión

Diseñada desde el inicio por investigadores y para investigadores.

Pensada para tus necesidades:

- Ahorra tiempo en la creación del proyecto y en la introducción de datos.
- Informes en tiempo real del desarrollo del proyecto.
- Exportación de los datos estructurada para su análisis.

Nuestro equipo cuenta con amplia experiencia en el sector de la programación, estructuración y codificación de datos, investigación médica y gestión de proyectos.

Esto hace que nuestra plataforma esté diseñada por y para investigadores.

Colaboramos con más de 200 centros de investigación, proporcionando una plataforma que facilita la recopilación y gestión eficiente de datos para proyectos sanitarios. Nuestra herramienta integra funciones diseñadas específicamente para fomentar la colaboración entre equipos, permitiendo un intercambio fluido de información y conocimientos.

5. Marco normativo

Se toma como referencia básica en materia de Seguridad de la Información la normativa siguiente:

- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Real Decreto ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
- Ley 9/2014, de 9 de mayo, de Telecomunicaciones.
- Reglamento (UE) 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 (Reglamento Europeo eIDAS).
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

6. Principios básicos

Los principios básicos son las directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

6.1. Seguridad como proceso integral

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

6.2. Gestión de la seguridad basada en 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.

6.3. Prevención, detección, respuesta y conservación

6.3.1. Prevención

PINVESTIGA debe evitar, o al menos prevenir en la medida de lo posibles, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evolución de amenazas y riesgos. Estos controles, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

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

6.3.2. Detección

PINVESTIGA, establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo dispuesto en el artículo 10 del ENS (vigilancia continua y reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS, Existencia de líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente

6.3.3. Respuesta

PINVESTIGA:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa puntos de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establece protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

6.3.4. Recuperación

Para garantizar la disponibilidad de los servicios, **PINVESTIGA,** dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

6.4. Existencia de líneas de defensa

El sistema de información dispondrá de una estrategia de protección constituida por diferentes capas, de forma que cuando una de las capas sea comprometida, permita desarrollar una acción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad del que el sistema sea comprometido en su conjunto, minimizando el impacto final sobre el mismo.

Existirán líneas de defensa constituidas tanto por medidas organizativas, físicas y lógicas.

6.5. Vigilancia continua y reevaluación periódica

PINVESTIGA llevará a cabo una vigilancia continua que permita la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permite a **PINVESTIGA** medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. **PINVESTIGA** reevaluará y actualizará periódicamente las medidas de seguridad, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

6.6. Diferenciación de responsabilidades

PINVESTIGA tendrá en cuenta la diferenciación de responsabilidades en su sistema de información siempre que sea posible. El detalle de las atribuciones de cada responsable, los mecanismos de coordinación y la resolución de conflictos se detallarán a lo largo de la presente política de seguridad.

7. Requisitos mínimos

Esta política de seguridad de la Información complementa las políticas de seguridad de **PINVESTIGA** en materia de protección de datos de carácter personal.

Esta Política de Seguridad de seguridad se desarrollará aplicando los siguientes requisitos mínimos:

- Organización e implantación del proceso de seguridad, de acuerdo al marco organizativo definido en el **apartado 8 de esta Política.**
- Análisis y gestión de los riesgos, de acuerdo a lo previsto en el procedimiento **PO.SEG.01 Categorización y Análisis de Riesgos.**
- Gestión de personal, de acuerdo a lo previsto en el procedimiento **PO.SEG.11 Gestión de personal y formación.**
- Profesionalidad, de acuerdo a lo previsto en el procedimiento **PO.SEG.11 Gestión de personal y formación**.
- Autorización y control de los accesos, de acuerdo a lo previsto en el procedimiento **PO.SEG.05 Control de accesos.**
- Protección de las instalaciones, de acuerdo a lo previsto en el procedimiento **PO.SEG.07 Seguridad Física**.
- Adquisición de productos, de acuerdo a lo previsto en el procedimiento **PO.SEG.03 Gestión de proveedores.**
- Seguridad por defecto, de acuerdo a lo previsto en el procedimiento **PO.SEG.12 Protección de equipos.**
- Integridad y actualización del sistema, de acuerdo a lo previsto en el procedimiento **PO.SEG.12 Protección de equipos.**
- Protección de la información almacenada y en tránsito, de acuerdo a lo previsto en el procedimiento **PO.SEG.15 Protección de la información**
- Prevención ante otros sistemas de información interconectados, de acuerdo a lo previsto en el procedimiento **PO.SEG.14 Seguridad de comunicaciones y servicios.**
- Registro de actividad, de acuerdo a lo previsto en el procedimiento **PO.SEG.02 Gestión de registros de actividad.**
- Incidentes de seguridad, de acuerdo a lo previsto en el procedimiento **PO.SEG.06 Gestión de incidentes**.
- Continuidad de la actividad, de acuerdo a lo previsto en el procedimiento **PO.SEG.09 Análisis de impacto**
- Mejora continua del proceso de seguridad, de acuerdo a lo previsto en el procedimiento **PO.SEG.16 Gestión del SGSI.**

8. Organización de la seguridad

La implantación de la Política de Seguridad en **PINVESTIGA** requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol especifico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

a) El Comité de Seguridad de la Información

b) Responsables del Servicio

c) Responsables de la Información

d) Responsable de Seguridad de la Información

e) Responsable de Sistemas

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles.

8.1. Comité de seguridad de la información

El Comité de Seguridad de la Información coordina la seguridad de la información en **PINVESTIGA**. Dicho Comité está compuesto por cada una de las figuras anteriormente mencionadas.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión y aprobación de la Política de Seguridad de la Información y de las responsabilidades principales;
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinados a garantizar la Seguridad de dicho activos;
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
    - Principales incidencias en la Seguridad de la Información;
    - Elaboración y actualización de planes de continuidad
    - Cumplimiento y difusión de las Políticas de Seguridad
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

8.1.1. Responsable de la Información

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos
- Determina los niveles de seguridad de la información.

8.1.2. Responsable del Servicio

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de los servicios prestados.
- Determina los niveles de seguridad de la información.

8.1.3. Responsable de Seguridad de la Información

Responsable de la definición, coordinación, implantación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo a los objetivos estratégicos de la organización.

El Responsable de Seguridad es el Punto de Contacto **(PoC).**

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de **PINVESTIGA**.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
    - La estrategia de seguridad de la información definida por el Comité de Seguridad.
    - Las normas y procedimientos contenidos en la Política de Seguridad de la Información de **PINVESTIGA** y normativa de desarrollo.
- Supervisar (como responsable último) los incidentes de seguridad informática producidas en **PINVESTIGA.**
- Difundir en **PINVESTIGA** las normas y procedimientos contenidos en la Política de Seguridad de la Información de **PINVESTIGA** y normativa de desarrollo, así como las funciones y obligaciones de todo **PINVESTIGA** en materia de seguridad de la información.
- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables tales como el RGPD.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de **PINVESTIGA.**

8.1.4. Responsable del Sistema

Es responsable último de asegurar la ejecución de medidas para asegurar los activos y servicios de los Sistemas de Información, que soportan la actividad de **PINVESTIGA**, de acuerdo a los objetivos estratégicos de **PINVESTIGA**.

Las funciones del Responsable de Sistemas de la Información son las siguientes:

- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos de **PINVESTIGA**, conforme a la estrategia de seguridad definida.
- Establecer la actuación de los Responsables Técnicos Informáticos, en los distintos entornos de seguridad que se designen.
- Garantizar la actualización del inventario de activos de Sistemas de Información de **PINVESTIGA.**
- Asegurar que existe el nivel de seguridad informática adecuado para cada uno de los activos inventariados, coordinando el correcto desarrollo, implantación, adecuación y operación de los controles y medidas destinados a garantizar el nivel de protección requerido.
- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en **PINVESTIGA**.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.
- Mantener y actualizar las directrices y políticas de seguridad de los Sistemas de Información y normativa asociada.

8.2. Procedimientos de designación

Se designan las siguientes responsabilidades:

- **Responsable del Servicio: Iván Fernández Rivas**
- **Responsable de la Información: Iván Fernández Rivas.**
- **Responsable de Seguridad: Sergio Martínez Portela**
- **Responsable del Sistema: Rubén Lino Mandado**

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

El Responsable de Seguridad de la Información será nombrado por la Dirección a propuesta del Comité de Seguridad.

8.3. Resolución de conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa, éste será resuelto por el superior jerárquico de los mismos con la mediación del Responsable de Seguridad, elevándose para su resolución a la Dirección en caso de no llegar a un acuerdo.

En la resolución de estas controversias se tendrán siempre en cuenta las exigencias derivadas de la protección de datos de carácter personal.

9. Revisión de la política de seguridad de la información

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

10. Datos de carácter personal

PINVESTIGA trata datos de carácter personal.

Todos los sistemas de información de **PINVESTIGA** se ajustarán a los niveles de seguridad requeridos por la normativa vigente en materia de Protección de Datos de Carácter Personal, identificada en el apartado **5. Marco Normativo**, de la presente Política de Seguridad de la Información.

11. Gestión de riesgos

Para todos los sistemas sujetos a esta Política de Seguridad de la Información debe realizarse periódicamente una evaluación de los a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información gestionada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información gestionados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

12. Estructuración de la documentación

Las directrices para la estructuración, gestión y acceso a la documentación de seguridad del SGSI de **PINVESTIGA**, se definen en el procedimiento "**PO.SEG.16 Gestión del SGSI**".

Se ha establecido un marco normativo en materia de seguridad de la información estructurado en diferentes niveles, de forma que los principios y los objetivos marcados en la política de seguridad de la institución tengan un desarrollo específico:

- Primer nivel: la presente Política de Seguridad de la Información, que debe ser aprobada por la Dirección a propuesta del Comité de Seguridad.
- Segundo nivel: la normativa de seguridad de la información aprobada por la Dirección. En ella se establecerán unas normas de uso aceptable de los sistemas de información.
- Tercer nivel: los procedimientos de seguridad de la información, en los que se detallará la manera correcta de realizar determinados procesos de modo que se proteja en todo momento la seguridad y la información. Estos procedimientos han de ser aprobados por el Comité de Seguridad.
- Cuarto nivel: estándares de seguridad, instrucciones técnicas, buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc. Ha de ser aprobada por el Comité de Seguridad.

Los documentos que integran el SGSI se encuentran, en soporte digital, a disposición de todo el personal al que le sea necesario para el desempeño de las funciones relacionadas con su puesto de trabajo. Estará disponible para su consulta, sin posibilidad de modificación.

13. Calificación de la información

Para calificar la información de **PINVESTIGA** atenderá a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas.

Tanto el responsable de cada información manejada por el sistema como los criterios de calificación de la información, que determinarán el nivel de seguridad requerido, se establecen en el procedimiento **PO.SEG.10 Clasificación de la información.**

14. Obligaciones del personal

Todos y cada uno de los usuarios de los sistemas de información de **PINVESTIGA** son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Todos los miembros de **PINVESTIGA** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de **PINVESTIGA** recibirán formación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **PINVESTIGA**, en particular a los de nueva incorporación.

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

14.1. Incumplimiento

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

15. Terceras partes

Las empresas y organizaciones externas que, con ocasión de su colaboración con **PINVESTIGA** para la prestación de un servicio, accedan o gestionen activos de información de **PINVESTIGA** o de sus usuarios, directa o indirectamente (en sistemas propios o ajenos), comparten la responsabilidad de mantener la seguridad de los sistemas y activos de **PINVESTIGA**, por lo que deberán asumir las siguientes obligaciones:

- No difundir ninguna información relativa a los servicios proporcionados a **PINVESTIGA** sin autorización expresa para ello.
- Informar y difundir a su personal las obligaciones establecidas en esta Política.
- Aplicar las medidas estipuladas por RGPD en el tratamiento de los datos personales responsabilidad de **PINVESTIGA** que traten por razón de la prestación del servicio.
- Aplicar los procedimientos para la gestión de seguridad relacionados con los servicios proporcionados a **PINVESTIGA**. Especialmente se deben aplicar los procedimientos relacionados con la gestión de usuarios, tales como notificaciones de altas y bajas, identificación de los usuarios, gestión de contraseñas, etc., en el sentido descrito en la presente política y normativa reguladora que sea de aplicación.
- Notificar cualquier incidencia o sospecha de amenaza a la seguridad de algún sistema o activo de **PINVESTIGA** a través de los mecanismos que se determinen, colaborando en la resolución de las mismas relacionados con los sistemas, servicios o personal de la propia entidad.
- Implantar medidas en sus propios sistemas y redes para prevenir la difusión de virus y/o código malicioso a los sistemas de **PINVESTIGA**. Específicamente, cualquier equipo conectado a la red corporativa de **PINVESTIGA** debe disponer de un antivirus actualizado preferiblemente de forma automática.
- Implantar medidas en sus propios sistemas y redes para prevenir el acceso no autorizado a los sistemas de **PINVESTIGA** desde otras redes. Entre otros, se deben aplicar las actualizaciones de seguridad en sus sistemas y se debe mantener un sistema cortafuegos para proteger las conexiones desde Internet y otras redes no confiables.

PINVESTIGA se reserva el derecho de revisar la relación con la entidad externa en caso de incumplimiento de las anteriores obligaciones.

Dirección: Iván Fernández Rivas	Firma: Fecha: 13/11/2025