INDICE:

Elaborado	Revisado y aprobado
Responsable del Sistema	*Gerente*

1 MISIÓN Y OBJETIVOS

La Dirección de PROMEDE, consciente del compromiso que contrae con sus clientes, la importancia del cuidado de la seguridad integral ha establecido en su organización un Sistema de Gestión de la Seguridad de la Información basado en el 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, atendiendo a los siguientes objetivos:

- PROMEDE, 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 o los servicios prestados.
- El objetivo de PROMEDE es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.
- Los sistemas TIC de PROMEDE 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 implica que los departamentos 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 servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.
- Los diferentes departamentos de PROMEDE deben 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 departamentos de PROMEDE deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 7 del ENS.
- El objetivo último de la seguridad de la información de PROMEDE es asegurar que una organización pueda cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:
    - Seguridad como un proceso integral y seguridad por defecto.
    - Reevaluación periódica e integridad y actualización del sistema.
    - Gestión de personal y profesionalidad.
    - Gestión de la seguridad basada en los riesgos y análisis y gestión de los riesgos.
    - Incidentes de seguridad, prevención, reacción y recuperación.
    - Líneas de defensa y prevención ante otros sistemas interconectados.

- Función diferenciada y organización e implantación del proceso de seguridad.
- Autorización y control de accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Protección de la información almacenada y en tránsito y continuidad de la actividad.
- Registros de actividad.

2 ALCANCE

PROMEDE aplicará la presente Política de Seguridad de la Información sobre aquellos sistemas que están relacionados con el ejercicio de desarrollo de las aplicaciones utilizadas dentro de su actividad.

De forma concreta, la presente Política de Seguridad es aplicable sobre las TIC y **los sistemas de información que dan soporte a los servicios de peritación y resolución extrajudicial sanitaria, valoración del daño corporal, defensor del asegurado y formación sobre la actividad a abogados o profesionales sanitarios, según el documento de categorización vigente.**

La organización desestima la aplicación de la presente Política de Seguridad de la Información sobre aquellos sistemas de información no reflejados en este apartado.

3 MARCO NORMATIVO

- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 y su modificación según el Real Decreto 951/2015, de 23 de octubre (se tendrá en cuenta el último texto consolidado).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la Información y Comercio Electrónico (LSSI).
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
- REGLAMENTO (UE) N o 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

4 ROLES Y RESPONSABILIDADES

- **El Responsable de la Información** será el propietario de la misma y tendrá las siguientes funciones:
    - Establecer y aprobar los requisitos de seguridad aplicables a la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad y/o Comité de Seguridad de la Información.
    - Aceptar los niveles de riesgo residual que afecten a la Información.
- **El Responsable del Servicio** será quien determine los requisitos de los servicios prestados, en consonancia, tendrá las siguientes funciones:
    - Establecer y aprobar los requisitos de seguridad aplicables al servicio dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad y/o Comité de Seguridad de la Información.
    - Aceptar los niveles de riesgo residual que afecten al Servicio.
- **El Responsable de Seguridad** será quien tome las decisiones adecuadas para satisfacer los requisitos de seguridad de la información y de los servicios. Dispondrá de las siguientes funciones:
    - Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
    - Promover la formación y concienciación en materia de seguridad de la información.
    - Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad; identificar medidas de seguridad; determinar configuraciones necesarias; elaborar documentación del sistema.
    - Proporcionar asesoramiento para la determinación de la categoría del sistema en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información.
    - Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
    - Gestionar las revisiones externas o internas del sistema.
    - Gestionar los procesos de certificación.
    - Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

- **El Responsable del Sistema**, dentro de sus áreas de actuación, tendrán asignadas las siguientes funciones:
    - Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
    - Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
    - Elaborar los procedimientos operativos necesarios.
    - Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
    - Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
    - Prestar al Responsable de Seguridad y/o el Comité de Seguridad asesoramiento para la determinación de la Categoría del Sistema.
    - Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
    - Llevar a cabo las funciones del administrador de la seguridad del sistema:
        - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
        - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
        - Aprobar los cambios en la configuración vigente del Sistema de Información.
        - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
        - Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
        - Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
        - Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
- **El Comité de Seguridad de la Información** alcanza a toda la empresa, es el mecanismo de coordinación y resolución de conflictos, entre otras funciones:
    - Atender las solicitudes, en materia de Seguridad de la Información, de la organización y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.

- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
  - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
  - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
  - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
  - Realizar un seguimiento de los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones respecto de ellos.
  - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
  - Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
  - Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con Dirección.
  - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
  - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
  - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
  - Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

La responsabilidad general de la seguridad de la información recaerá sobre el Responsable de Seguridad, siendo la responsabilidad última del Comité de Seguridad de la Información y de la Dirección como máximo Responsable del Sistema de gestión de seguridad de la

información. El detalle de la composición del Comité de Seguridad de la Información, así como las obligaciones de cada rol en el ámbito de la seguridad de la información se determina actas del propio comité.

Es función de la Dirección de PROMEDE designar al:

- Responsable de la Información.
- Responsable del Servicio (puede ser el mismo que el Responsable de la información).
- Responsable de Seguridad.
- Responsable del Sistema.

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

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Responsable de Seguridad.

Por la presente, la Dirección de PROMEDE asume la responsabilidad final y última del cumplimiento de la política.

5 REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad de la Información 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 Dirección y difundida para que la conozcan todas las partes afectadas.

6 DATOS DE CARÁCTER PERSONAL

PROMEDE solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

A la vista de la entrada en aplicación, el día 25 de mayo de 2018, del 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) y su traslación a la legislación española con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se han ido adaptando las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de

riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos.

Del mismo modo, se deberá de garantizar el cumplimiento de la política de protección de datos establecida por PROMEDE.

7 GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la tipología de la información manejada.
- 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 de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. 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.

8 OBLIGACIONES DEL PERSONAL

Todos y cada uno de los usuarios de los sistemas de información de PROMEDE 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 PROMEDE 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 de la Información disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de PROMEDE recibirán formación en seguridad de la información. Se establecerá un programa de concienciación continua para atender a todos los miembros de PROMEDE, 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.

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.

9 TERCERAS PARTES

Cuando PROMEDE 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 reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando PROMEDE 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 ataña a dichos servicios o información. Dicha tercera parte quedará 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 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 antes de seguir adelante.

FIRMADO: