h) Colaborar con la AEAD en la detección, diagnóstico y resolución de las incidencias técnicas, incluyendo, en su caso, la realización de actuaciones que aseguren la reducción del tiempo de resolución de las incidencias.

i) Seguir los procedimientos establecidos para armonizar los procesos de administración de aplicaciones y sistemas usuarios de las soluciones tecnológicas incluidas en el presente Convenio.

j) Adoptar y cumplir las medidas de seguridad para proteger debidamente la información y los sistemas asociados a las soluciones tecnológicas incluidas en el presente Convenio, atendiendo al Real Decreto 311/2022, de 3 de mayo, y a las correspondientes Declaraciones de Aplicabilidad de las citadas soluciones.

k) Cumplir las obligaciones que le corresponden como responsable del tratamiento de datos personales, de acuerdo con lo establecido en la cláusula decimocuarta del presente convenio en aplicación de lo previsto en el Reglamento general de protección de datos, y en la Ley Orgánica 3/2018, de 5 de diciembre.

l) Cumplir y velar por el cumplimiento de las Normas Técnicas de Interoperabilidad previstas en la disposición adicional primera del 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 que se encuentren vigentes en cada momento y sean aplicables a cada solución tecnológica.

m) Asignar responsables del uso de los servicios que determinarán las condiciones y normas aplicables a usuarios y aplicaciones.

n) Tramitar las autorizaciones que se den a los usuarios, y realizar la gestión de los usuarios de las soluciones en su ámbito de competencia.

2. La Ciudad Autónoma de Melilla y los sujetos que en su caso se adhieran a este convenio, asumen las siguientes obligaciones específicas respecto a soluciones tecnológicas concretas:

a) En lo que concierne a la Red de Comunicaciones de las Administraciones Públicas (Red SARA), ejercer sus funciones como Proveedor de Acceso a la Red SARA (PAS) para sus órganos y los sujetos adheridos, de acuerdo con lo previsto en la Norma Técnica de Interoperabilidad de requisitos de conexión a la Red de las Administraciones Públicas aprobada por Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública.

b) En lo que concierne a los sistemas de identificación y firma de las Administraciones Públicas y el proceso de emisión y gestión de las correspondientes credenciales de acceso:

1st. Poner a disposición de los ciudadanos oficinas de registro presencial para facilitar la emisión de credenciales de identidad en Cl@ve o realizar cualquier otra gestión al respecto de esas credenciales.

2nd. Participar, en los procesos de emisión y gestión de credenciales mediante sistemas de identificación remota por vídeo que se habiliten al respecto. Los empleados públicos que participen en dichos procesos se encargarán de validar y/o verificar los datos suministrados por los ciudadanos de modo que sea posible la emisión de credenciales.

Los condicionantes que deberán satisfacer para cumplir las anteriores obligaciones se mantendrán actualizados en el Portal de Administración Electrónica y se adecuarán a las necesidades estimadas para periodos de un año. Dichos condicionantes se determinarán en función de, entre otros parámetros, la población atendida, el número anual de identificaciones y firmas que realice el organismo y el tamaño del organismo.

c) En lo que concierne al servicio AutenticA, designar una o más personas como administradores delegados de AutenticA, para la gestión de usuarios de las soluciones tecnológicas previstas en la cláusula Segunda que requieran este servicio.

d) En lo que concierne a la Plataforma de Intermediación de datos de la Administración General del Estado para la verificación y consulta de datos y Portfolio SCSP:

1st. Respetar todos los condicionantes establecidos en el estándar definido en la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos aprobada por Resolución de 28 de junio de 2012 de la Secretaría de Estado de Administraciones Públicas, así como en las especificaciones del protocolo SCSP.

2nd. Gestionar las autorizaciones de usuarios que se soliciten, de acuerdo con el modelo de gobernanza definido en la Norma técnica de Interoperabilidad de Protocolos de intermediación de datos en la que se regulan las responsabilidades de los requirentes y cesionarios de los servicios y atendiendo a las condiciones específicas determinadas por los cedentes de datos que se recogen en los manuales de procedimiento de autorización y acceso a los servicios disponibles en el PAe.

3rd. Recoger la finalidad concreta por la que se realiza cada consulta y acceso a la información de acuerdo con el modelo de gobernanza establecido.

4th. Velar por la plena validez de los datos y documentos aportados por este servicio, de acuerdo con lo establecido en la normativa de aplicación.

5th. Garantizar el cumplimiento de las medidas de seguridad y requisitos de autenticidad, confidencialidad, integridad, trazabilidad, auditoría e interoperabilidad para todos los datos intermediados, sea como emisores o como requirentes de los mismos.

6th. Facilitar el acceso de los órganos de las Administraciones Públicas, o sus organismos públicos o entidades de derecho público vinculados o

dependientes a los documentos y datos que obren en poder de la Ciudad Autónoma o de los sujetos adheridos y sean necesarios para el desarrollo de los procedimientos administrativos tramitados por los anteriores en el ejercicio de sus competencias.

e) En lo que concierne al Sistema de Interconexión de Registros (SIR):

1st. Cumplir con los procedimientos establecidos en la Guía Funcional para las Oficinas de Asistencia en Materia de Registro SIR, publicada en el PAe.

2nd. Coordinar con la AEAD la gestión del cambio de las instalaciones certificadas y adaptarlas a las nuevas funcionalidades de la plataforma SIR, para garantizar que no impactan en la interoperabilidad con el sistema y, en su caso, realizar nueva certificación completa de la aplicación. En todo caso, la AEAD determinará aquellos supuestos en los que admitirá solicitudes de certificación de soluciones de registro.