I - JUNTAS GENERALES DE ÁLAVA Y ADMINISTRACIÓN FORAL DEL TERRITORIO HISTÓRICO DE ÁLAVA

Diputación Foral de Álava

DEPARTAMENTO DE EMPLEO, COMERCIO, TURISMO Y ADMINISTRACIÓN FORAL

Decreto Foral 27/2026, de 28 de julio, del Consejo de Gobierno Foral. Aprobar la política de protección de datos personales y de seguridad de la información de la Diputación Foral de Álava

El 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 y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD) establece en su artículo 24, dentro de las obligaciones generales de la persona responsable del tratamiento de datos personales que, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, la persona responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el citado reglamento. Asimismo, dispone que dichas medidas se revisarán y actualizarán cuando sea necesario y que, cuando sean proporcionadas en relación con las actividades de tratamiento, entre dichas medidas se incluirá la aplicación por parte de la persona responsable del tratamiento de las oportunas políticas de protección de datos.

En el mismo sentido, el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD) establece como obligaciones generales, tanto para la persona responsable del tratamiento como para el encargado, y teniendo en cuenta lo establecido en los artículo 24 y 25 del RGPD, que éstas determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el RGPD, con la LOPDGDD, sus normas de desarrollo y la legislación sectorial aplicable.

Por su parte, el artículo 13 de la Ley 39/2015, de 1 de octubre, de procedimiento administrativo común de las Administraciones Públicas, relativo a los derechos de las personas en sus relaciones con las Administraciones Públicas, contempla expresamente el derecho a la protección de datos personales y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Además, el artículo 3.2 de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público dispone que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos personales y facilitarán preferentemente la prestación conjunta de servicios a las personas interesadas. En este sentido, el artículo 156 de esta Ley dispone que el Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de los medios electrónicos en el sector público, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) en el ámbito de la Administración electrónica establece que las Administraciones Públicas deben aplicar medidas de seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades

D.L.: VI-1/1958 ISSN: 2254-8432

reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados. En este ámbito, la política de seguridad de la información constituye el marco de referencia orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad establecidos en el ENS.

Considerando la íntima conexión entre ambas materias, esto es, la protección de datos personales y la gestión de la seguridad de la información, así como la obligación de establecer políticas para cada ámbito, se considera conveniente adoptar una política conjunta de protección de datos y seguridad de la información. Así pues, la política de protección de datos y de seguridad de la información es el documento base mediante el cual se define el marco de referencia que permite la gestión de la protección de datos y de la seguridad de la información en el contexto de las actividades de tratamiento con datos personales y los sistemas de información de la Diputación Foral de Álava.

El presente decreto foral se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015 y recogidos en el artículo 3 del Decreto Foral 6/2023, de 28 de febrero, que aprueba el procedimiento de elaboración de disposiciones de carácter general de la Diputación Foral de Álava. En particular, los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia.

Así, en los antecedentes expuestos se ha justificado suficientemente la necesidad de la aprobación de una nueva política de protección de datos y seguridad de la información, siendo además el instrumento más adecuado para garantizar su consecución y una actuación normativa proporcionada, ya que se limita al mínimo imprescindible para conseguir el fin perseguido. Se garantiza igualmente el principio de seguridad jurídica, derogando expresamente los Acuerdos que aprobaban la anterior política de seguridad y de estructura de seguridad en materia de protección de datos de la Diputación Foral de Álava. Respecto al principio de transparencia, no se ha vulnerado el mismo ya que, al ser contenido puramente organizativo, es posible prescindir de los trámites de consulta pública previa y de audiencia e información pública, ordenándose, en todo caso, su publicación en el BOTHA inmediatamente después de su aprobación. En cuanto al principio de eficiencia, la regulación planteada no implica cargas administrativas ni innecesarias para la ciudadanía. En relación con los principios de simplicidad y comprensibilidad, el texto propuesto ha sido redactado de forma estructurada y utilizando un lenguaje claro y fácilmente comprensible.

En su virtud, a propuesta conjunta de la Diputada foral de Empleo, Comercio y Turismo y de Administración Foral y del Diputado foral de Igualdad, Euskera y Gobernanza, previa deliberación del Consejo de Gobierno Foral en sesión celebrada en día de hoy,

DISPONGO

Artículo 1. Objeto y ámbito de aplicación

1. El presente Decreto Foral tiene por objeto aprobar la política de protección de datos y seguridad de la información de la Diputación Foral de Álava, la cual constituye el conjunto de medidas técnicas y organizativas apropiadas para garantizar el cumplimiento de la normativa aplicable al tratamiento de los datos personales, así como los principios básicos y requisitos mínimos que permiten una protección adecuada de la información que se gestiona en el ámbito de la Diputación Foral de Álava.

2. Esta Política será de aplicación a todos los sistemas de información y a todas las actividades de tratamiento de datos personales de los que sean responsables la Diputación Foral de Álava.

3. Esta Política será de obligado cumplimiento para todas las unidades que conforman la estructura orgánica de la Diputación Foral de Álava. El resto del sector público foral de Álava se podrá adherir a la presente Política de protección de datos y seguridad de la información mediante la formalización del protocolo de adhesión que se incorpora como anexo I.

D.L.: VI-1/1958 ISSN: 2254-8432

4. La protección de datos personales y la seguridad de la información compromete y obliga a todo el personal de la Diputación Foral de Álava, así como a terceras personas que presten servicios a ésta, o que se relacionen con la misma mediante la correspondiente relación jurídica.

5. En el ámbito de aplicación material del RGPD y el ENS, la presente Política afectará a la información tratada por cualquier medio que gestione la Diputación Foral de Álava en el ejercicio de sus competencias, con independencia del soporte.

Artículo 2. Marco normativo

1. Esta Política se fundamenta en la siguiente legislación y normas aplicables:

— Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.

— 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 (RGPD).

— 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 y por la que se deroga la Directiva 1999/93/CE.

— Ley de Orgánica 3/2018, de 5 de diciembre, de Protección de datos Personales y garantía de los derechos digitales (LOPDyGDD).

— Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

— Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos.

— 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.

— 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.

— Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

— Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

— 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.

— 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.

— Norma Foral 1/2017, de 8 febrero, de transparencia, participación ciudadana y buen gobierno del sector público del Territorio Histórico de Álava.

— Decreto 91/2023, de 20 de junio, de atención integral y multicanal a la ciudadanía y acceso a los servicios públicos por medios electrónicos.

— Estándares internacionales de gestión de la seguridad (ISO/IEC 27001:2022, 27002:2022, 31000:2010, 22301:2020, NIST SP 800-53).

— Resto de normativa que resulte de aplicación.

2. Las normas que integran este marco normativo se recogen en un registro a tales efectos, el cual se mantendrá actualizado.

D.L.: VI-1/1958 ISSN: 2254-8432

Artículo 3. Principios de protección de datos y seguridad de la información

La Diputación Foral de Álava tratará la información y los datos personales conforme a los siguientes principios de protección de datos y seguridad de la información:

1. Licitud, lealtad y transparencia: los datos personales serán tratados de manera lícita, leal y transparente con la persona interesada. Limitación de la finalidad: los datos personales serán tratados para el cumplimiento de fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

2. El tratamiento de datos personales con fines distintos de aquéllos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial y cumpliendo las condiciones y requisitos establecidos en la normativa de protección de datos.

3. Minimización de datos: los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

4. Exactitud: los datos personales serán exactos y, si fuera necesario, actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

5. Limitación del plazo de conservación: los datos personales serán mantenidos de forma que se permita la identificación de las personas interesadas durante no más tiempo del necesario para los fines que justificaron su tratamiento.

6. Integridad y confidencialidad: los datos personales serán tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

7. Quienes intervengan en el tratamiento de los datos estarán sujetos al deber de secreto incluso después de haber concluido la relación que justificaba su intervención.

8. Responsabilidad proactiva: la Diputación Foral de Álava será responsable del cumplimiento de los principios referenciados en este artículo y adoptará las medidas organizativas, operacionales y técnicas que le permitan estar en condiciones de demostrar dicho cumplimiento.

9. Atención a los derechos de las personas afectadas: se adoptarán medidas en la organización que garanticen el adecuado ejercicio por las personas afectadas, cuando proceda, de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad respecto de sus datos personales.

10. Alcance estratégico: la protección de datos y la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas de la Diputación Foral de Álava, para conformar un todo coherente y eficaz.

11. Responsabilidad diferenciada: en los sistemas de información responsabilidad de la Diputación Foral de Álava se observará el principio de responsabilidad diferenciada, de forma que se delimiten las diferentes responsabilidades y roles:

a. Responsable de tratamiento: la persona que determina los fines y medios del tratamiento.

b. Encargado de tratamiento: la persona que trata los datos personales por cuenta del responsable del tratamiento según sus requerimientos.

c. Delegada o delegado de protección de datos: la persona que informa y asesora al responsable del tratamiento de las obligaciones en materia de cumplimiento de RGPD.

D.L.: VI-1/1958 ISSN: 2254-8432

d. Responsable de la información: la persona que determina los requisitos de seguridad de la información tratada.

e. Responsable del servicio: la persona que determina los requisitos funcionales y de seguridad de los servicios prestados a partir de la información.

f. Responsable de seguridad de la información: la persona que determina las decisiones para satisfacer los requisitos de seguridad.

g. Responsable del sistema: la persona que tiene la responsabilidad sobre los requisitos no funcionales y de diseño, construcción, operación y soporte de los sistemas de información utilizados en la prestación de los servicios.

12. Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos relacionados con los sistemas de información. La aplicación de la presente Política estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural. Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa vigente en materia de seguridad de la información y protección de datos personales.

13. Gestión de la seguridad basada en riesgos: el proceso de seguridad que protegerá los derechos y libertades de las personas interesadas, así como los activos de la Diputación Foral de Álava se basarán en la gestión del riesgo que permita minimizarlo hasta niveles aceptables, manteniendo el equilibrio entre la funcionalidad, la naturaleza de los datos, los tratamientos y las medidas de control a aplicar.

14. Análisis y gestión de los riesgos: el análisis y gestión de los riesgos será parte esencial del proceso de seguridad y constituirá una actividad continua y permanentemente actualizada. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción de estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera proporcionada a la naturaleza de la información a tratar, de los servicios a prestar y de los riesgos a los que estén expuestos

15. Proporcionalidad: la Diputación Foral de Álava establecerá medidas de protección, detección y recuperación que resulten proporcionales a los potenciales riesgos y a la criticidad y el valor de la información, de los tratamientos de datos personales y de los servicios afectados.

16. Protección de datos y seguridad desde el diseño y por defecto: la Diputación Foral de Álava promoverá la implantación del principio de protección de datos desde el diseño y por defecto, de forma que la protección de datos y la seguridad de la información se encuentre presente desde el diseño y por defecto para todos los tratamientos de datos personales y los sistemas de información.

17. Proceso de verificación: la Diputación Foral de Álava implantará un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos.

18. Seguridad de los activos de información: se implantarán las medidas técnicas y organizativas necesarias para que las personas que tienen acceso a los activos de información y a los datos personales conozcan sus obligaciones y responsabilidades y, de este modo, se reduzca el riesgo derivado de un uso indebido de dichos activos.

19. Seguridad física: 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.

D.L.: VI-1/1958 ISSN: 2254-8432

20. Seguridad en la gestión de comunicaciones: 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.

21. Control de accesos: se limitará el acceso a los activos de información por parte de las 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.

22. Para corregir, o exigir responsabilidades en su caso, cada persona que acceda a la información del sistema debe estar identificada de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos y quién ha realizado determinada actividad.

23. Gestión de los incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro, resolución y notificación, en los términos previstos en la normativa de protección de datos y seguridad de la información, de los incidentes de seguridad.

24. Gestión de la continuidad: 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 con las necesidades de nivel de servicio de la Diputación Foral de Álava.

25. Adquisición, desarrollo y mantenimiento de los sistemas de información: se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

26. Cumplimiento: se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información y protección de datos personales.

Artículo 4. Política corporativa de protección de datos personales y de seguridad de la información

La política corporativa de protección de datos personales y de seguridad de la información de la Diputación Foral de Álava se aprueba y publica íntegramente como Anexo II a este Decreto Foral.

Artículo 5. Estructura organizativa

La estructura organizativa para la gestión de la seguridad de la información en el ámbito de la política de protección de datos y seguridad de la información se desarrolla en las figuras y roles descritos en el anexo III del presente Decreto Foral.

Artículo 6. Registro de las actividades de tratamiento

1. La Diputación Foral de Álava mantendrá actualizado el registro de las actividades de tratamiento de datos personales de las que sea responsable, que incluirá toda la información a la que se refiere el artículo 30 del RGPD. Las direcciones de los diferentes Departamentos, en calidad de responsables de tratamiento de los datos personales que realiza en ejercicio de sus competencias, tienen la obligación de documentar el citado registro.

2. El registro de las actividades de tratamiento se mantendrá continuamente actualizado y su inventario podrá consultarse en la página web corporativa, www.araba.eus.

D.L.: VI-1/1958 ISSN: 2254-8432

Artículo 7. Análisis de riesgos, evaluación de impacto en la protección de datos y gestión de los riesgos de seguridad de la información

1. Cuando la información contenga datos personales se llevará a cabo, de forma periódica, un análisis de riesgos que permita identificar y gestionar los riesgos minimizándolos hasta los niveles que puedan considerarse aceptables. Esta evaluación incluirá un análisis de los riesgos para los derechos y libertades de las personas físicas respecto de las actividades de tratamiento de datos personales, así como para los sistemas de información que sirven de soporte para dichas actividades de tratamiento. Asimismo, cuando del análisis realizado resulte probable que el tratamiento suponga un alto riesgo para los derechos y libertades de las personas, se llevará a cabo una evaluación de impacto en protección de datos personales, conforme a lo previsto en el artículo 35 del RGPD.

2. La gestión de riesgos de seguridad de la información debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y en la reevaluación periódica.

Artículo 8. Encargos de tratamiento

Son actos jurídicos que establecen la relación jurídica entre las personas responsables del tratamiento y las encargadas del tratamiento. Deben contener el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categoría de personas interesadas, las obligaciones y derechos de ambas partes, así como el resto de las cuestiones indicadas en el artículo 28 del RGPD. Los encargos de tratamiento establecerán las instrucciones necesarias para que las entidades que tratan datos personales por cuenta de la Diputación Foral de Álava respeten los siguientes requisitos:

— Que los datos personales se destinen a la finalidad de prestar el servicio encargado y no se destinen a finalidades diferentes e incompatibles a las expresamente autorizadas.

— Que los datos personales no se comuniquen a terceras personas o entidades sin base jurídica legitimadora, de conformidad con el artículo 6 del RGPD.

— Que se garantice la confidencialidad e integridad de los datos personales mediante la implantación de medidas de seguridad.

Artículo 9. Transparencia informativa

En cumplimiento del deber de transparencia, la Diputación Foral de Álava, cuando actúe como responsable del tratamiento, adoptará las medidas oportunas para facilitar a las personas físicas titulares de los datos toda la información indicada en los artículos 13 y 14 del RGPD. Esta información se facilitará de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

Artículo 10. Ejercicio de derechos

1. En cumplimiento de los artículos 15 a 22 del RGPD, la Diputación Foral de Álava garantizará el ejercicio de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento, derecho a no ser objeto de decisiones individuales automatizadas y portabilidad, en su caso.

2. El procedimiento a seguir para el ejercicio de derechos personales en la Diputación Foral de Álava es el siguiente:

a) Las solicitudes de ejercicio de derechos en materia de protección de datos personales podrán presentarse mediante modelo de solicitud habilitado, de la siguiente forma:

— Telemáticamente: en la sede electrónica de la Diputación Foral de Álava.

— Presencialmente: en las oficinas del Registro General de la Diputación Foral de Álava.

D.L.: VI-1/1958 ISSN: 2254-8432

b) El responsable del tratamiento dará respuesta a la solicitud sin dilación indebida y, en cualquier caso, en el plazo máximo de un mes, de acuerdo con el artículo 12.3 del RGPD. Este plazo será prorrogable por un plazo máximo de dos meses, teniendo en cuenta la complejidad y el número de solicitudes, de lo cual se informará a la persona afectada de forma motivada.

c) En caso de desestimación de la solicitud de ejercicio de derechos en materia de protección de datos personales, las personas afectadas podrán recabar la tutela del derecho ante la AVPD mediante la presentación de reclamación ante la misma o, en su caso, dirigir reclamación previa ante la persona delegada de protección de datos de la Diputación Foral de Álava, de conformidad con el artículo 37 de la LOPDGDD.

Artículo 11. Limitación del plazo de conservación de los datos personales

Los datos personales se conservarán, con carácter general, durante el tiempo necesario para la tramitación del procedimiento correspondiente a la actividad o servicio para los que se recaben y, además, al plazo de prescripción o caducidad posterior para la extinción de las posibles responsabilidades que pudieran derivarse del propio tratamiento.

Artículo 12. Protección de datos y seguridad desde el diseño y por defecto

La Diputación Foral de Álava aplicará las medidas técnicas y organizativas apropiadas para asegurar que los tratamientos de datos personales se configuren, por defecto, de forma que sólo se traten los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. En concreto, estas medidas se aplicarán a la cantidad de datos personales recogidos, la extensión del tratamiento, el plazo de conservación y la accesibilidad.

Las medidas de seguridad se incluirán por defecto, de manera que la seguridad de la información esté siempre presente en todos los sistemas que traten datos personales. En cuanto a dichas medidas de seguridad, se elegirán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, entre otras, la seudonimización, el cifrado y la anonimización de datos personales, tal y como establece el artículo 32 del RGPD.

Artículo 13. Notificación de brechas de seguridad de los datos personales e incidentes de seguridad

La Diputación Foral de Álava adoptará las medidas necesarias para garantizar la notificación a la autoridad de control y, en su caso, comunicación a las personas afectadas, de las brechas de seguridad de los datos personales que pudieran producirse a través del procedimiento establecido al efecto.

Artículo 14. Revisión y auditoría

La Diputación Foral de Álava llevará a cabo de forma periódica, en los plazos legalmente establecidos, una auditoría encaminada a la verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos y sistemas de información.

En todo caso, realizará una auditoría específica y extraordinaria cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

Artículo 15. Obligaciones del personal

El personal al servicio de la Diputación Foral de Álava prestará su colaboración en las actuaciones de implementación de la política de protección de datos y seguridad de la información.

Dicho personal tiene la obligación de conocer y cumplir lo previsto en la presente política, así como en las normas y procedimientos que la desarrollen.

D.L.: VI-1/1958 ISSN: 2254-8432

Artículo 16. Concienciación y formación

La Diputación Foral de Álava fomentará el desarrollo de planes de formación, enfocados y dirigidos a su personal para que reciban sesiones de concienciación en materia de protección de datos personales y seguridad de la información de manera periódica. En particular, se prestará especial atención a los siguientes ámbitos y objetivos:

a) Que se preste formación y concienciación a las nuevas incorporaciones de personal, y de forma periódica y continuada, a todo el personal de la Diputación Foral de Álava.

b) Que las personas con responsabilidad en el uso, operación o administración de sistemas reciban formación para el manejo seguro de los sistemas, en la medida en que la necesiten para desempeñar de forma eficaz y eficiente su trabajo.

c) Que la formación en protección de datos personales y seguridad de la información que se diseñe y apruebe para su impartición entre personal perteneciente a grupos específicos, que por las necesidades del puesto de trabajo necesiten adquirir conocimientos en la misma, tenga carácter preferente y en su caso, sea obligatoria al objeto de cubrir estas necesidades formativas en el desempeño de las funciones del puesto y la correcta asunción de las responsabilidades inherentes al mismo.

Disposición adicional única

El Cuerpo Documental de Seguridad de la Información se implementará a esta Política en el plazo máximo de seis meses desde su entrada en vigor.

Disposición derogatoria única

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en el presente Decreto Foral y, en particular, el Acuerdo 310/2008, de 20 de mayo, del Consejo, por el que se aprueba la política de seguridad y el documento de seguridad de la Diputación Foral de Álava y el Acuerdo 646/2018, de 27 de noviembre, del Consejo de Gobierno Foral, que aprueba la modificación del Acuerdo 480/2007, de 22 de mayo, que aprobó la estructura funcional para la seguridad de los ficheros de esta diputación afectados por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), a fin de adecuarlo al reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

Disposición final primera. Desarrollo normativo

Se faculta a la persona titular del Departamento de Empleo, Comercio y Turismo y de Administración Foral para adoptar las disposiciones necesarias para la ejecución y desarrollo del presente Decreto Foral. Asimismo, se le faculta de forma expresa a la persona titular del Departamento de del Empleo, Comercio y Turismo y de Administración Foral para la modificación, actualización y adaptación a la evolución tecnológica de las determinaciones relativas a la Política Corporativa de Seguridad de la Información y de la Organización de Seguridad de los Anexos de este Decreto Foral.

Se faculta a la persona titular de la Dirección de Servicios Generales para que dicte las circulares e instrucciones de servicio necesarias con el fin de garantizar la homogeneidad y la calidad.

D.L.: VI-1/1958 ISSN: 2254-8432

Disposición final segunda. Entrada en vigor

El presente Decreto Foral entrará en vigor el día siguiente al de su publicación en el BOTHA.

Vitoria-Gasteiz, 28 de julio de 2026

Diputado General
RAMIRO GONZÁLEZ VICENTE

Primera Teniente de Diputado General y Diputada Foral de Empleo, Comercio, Turismo y Administración Foral
CRISTINA GONZÁLEZ CALVAR

Diputado Foral de Igualdad, Euskera y Gobernanza
IÑAKI GURTUBAI ARTETXE

Director de Servicios Generales
IKER MIRANDA SERRANO

Directora de Gobernanza
MIREN ZABALA BASTERRECHEA

D.L.: VI-1/1958 ISSN: 2254-8432

ANEXO I. PROTOCOLO DE ADHESIÓN A LA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES Y DE SEGURIDAD DE LA INFORMACIÓN DE LA DIPUTACIÓN FORAL DE ÁLAVA

(Nombre y cargo)……, en representación de (organismo autónomo, sociedad pública o consorcio)……..,

EXPONE

Que el……..de (organismo autónomo, sociedad pública o consorcio) ha acordado, con fecha…….de……..…de……., solicitar la adhesión a la Política de protección de datos personales y seguridad de la información de la Diputación Foral de Álava.

En su virtud,

ACUERDA

Primero. Aprobar la adhesión (organismo autónomo, sociedad pública o consorcio) a la Política de protección de datos personales y seguridad de la información de la Diputación Foral de Álava, excepto a la estructura organizativa para la gestión de la seguridad de la información en el ámbito de la política de protección de datos y seguridad de la información, contenida en el anexo III del citado Decreto Foral.

Esta adhesión se entenderá realizada a la Política de protección de datos personales y seguridad de la información de la Diputación Foral de Álava que, en cada momento, se encuentre en vigor.

Segundo. Asumir las obligaciones establecidas en el Decreto Foral por el que se aprueba la Política de protección de datos personales y seguridad de la información de la Diputación Foral de Álava, y realizar las actuaciones previstas en el mismo para su adecuada gestión

Tercero. Designar las personas que realizarán las tareas de implementar, gestionar y llevar a cabo la coordinación interna de la Política de protección de datos personales y seguridad de la información de la Diputación Foral de Álava, y que actuarán como interlocutoras ante la DFA.

D.L.: VI-1/1958 ISSN: 2254-8432

(Nombre y apellidos de las personas interlocutoras del organismo autónomo, sociedad pública o consorcio)

- .....
- .....
- .....
- .....
- .....
- .....

Las variaciones en esa relación nominal deberán ser comunicadas a la mayor brevedad a la Dirección de Servicios Generales de la DFA.

(Lugar y fecha)

Nombre y apellidos	Nombre y apellidos
(Firma)	(Firma)
Director/a de Servicios Generales de la DFA	Cargo en representación de organismo autónomo, sociedad pública o consorcio

2

D.L.: VI-1/1958 ISSN: 2254-8432

Arabako Foru Aldundia
Diputación Foral de Álava

DCSGPOSEG - POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES Y DE SEGURIDAD DE LA INFORMACIÓN DE LA DIPUTACIÓN FORAL DE ÁLAVA

Clasificación del documento: Público

D.L.: VI-1/1958 ISSN: 2254-8432

Hoja de control:

Documento:	
Autor:	
Versión:	**Fecha de versión:**
Revisado por:	**Fecha de revisión:**
Aprobado por:	**Fecha de aprobación:**

Control de cambios:

Versión	Fecha	Elaborado por:	Descripción

Arabako Foru Aldundia
Diputación Foral de Álava

1. Exposición de Motivos

En el ámbito de las Administraciones Públicas, el derecho a comunicarse con ellas a través de medios electrónicos y el apoyo al desarrollo de la Sociedad de la Información, al que dichas Administraciones están obligadas, comporta el impulso de acciones que promuevan la consecución de dichos fines.

Por ello, las Administraciones Públicas deben crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de la implantación de las medidas necesarias para garantizar la seguridad de los sistemas de información, de la integridad de los datos (con especial incidencia en los datos personales), de las comunicaciones y los servicios electrónicos, facilitando así a la ciudadanía, empresas y a otras Administraciones Públicas, el ejercicio de los derechos y el cumplimento de los deberes a través de estos medios.

Además, las Administraciones Públicas están especialmente sujetas a riesgos debido a su naturaleza y misión, por lo que el desarrollo eficaz de sus funciones requiere la adopción de un conjunto amplio de medidas dirigidas a proteger de forma prioritaria:

- Las tecnologías y los sistemas informáticos que permiten el tratamiento y difusión de la información, así como la gestión ágil y eficaz del servicio.

- La continuidad de la operativa permitiendo proporcionar el servicio requerido en el momento adecuado a los destinatarios del mismo.

2. Objeto y ámbito de aplicación

2.1. Propósito de la Política Corporativa de Protección de Datos Personales y de Seguridad de la Información

Promover e impulsar la consecución de los principios básicos de seguridad de la información y los sistemas en el ámbito de la Diputación Foral de Álava (en adelante DFA).

Establecer las directrices para la implantación de medidas organizativas, técnicas, físicas y legales destinadas a la protección de los sistemas de información.

Garantizar el cumplimento de la legislación actual siendo de aplicación en el contexto de la seguridad de la información, y preservar en todo momento la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la misma.

2.1. Ámbito de aplicación de la Política Corporativa de Protección de Datos Personales y de Seguridad de la Información

La presente política es de aplicación obligatoria para la Diputación Foral de Álava (DFA). Asimismo, el resto del sector público foral de Álava se podrá adherirse a la Política Corporativa de Protección de Datos Personales y de Seguridad de la Información mediante la formalización del convenio de adhesión.

D.L.: VI-1/1958 ISSN: 2254-8432

2.2. Marco de aplicación de la Política Corporativa de Protección de Datos Personales y de Seguridad de la Información

La Política Corporativa de Protección de Datos Personales y de Seguridad de la Información establece las directrices de Seguridad de la Información que con carácter general son de aplicación en la DFA, considerando las mismas como mínimos exigibles, y faculta la creación en entornos particulares de la DFA de Políticas de Seguridad complementarias, siempre que las mismas tengan un carácter más restrictivo que la establecida a nivel corporativo. Por ello la presente Política constituye el marco de referencia en relación con el cual deberán alinearse las diversas Políticas de Seguridad de la Información que se establezcan dentro de dichos ámbitos particulares.

2.3. Revisión y vigencia

La presente política permanecerá en vigor hasta su actualización formal, y será objeto de una revisión cada vez que se produzcan modificaciones relevantes que afecten al contenido de la misma.

3. Referencias de implementación

La Política Corporativa de Protección de Datos Personales y de Seguridad de la Información de la Diputación Foral de Álava (DFA) se fundamenta en las directrices y principios establecidos en el Esquema Nacional de Seguridad (en adelante, ENS). Asimismo, han sido tomadas en consideración, y deberán seguir siéndolo en el futuro, las normativas y estándares de aplicación pertinentes, con el fin de adecuar dicha Política a los requisitos normativos, reglamentarios y de buenas prácticas que de ellos se deriven.

La identificación, revisión y actualización de la legislación aplicable en materia de seguridad y privacidad de la información se articulará a través del procedimiento denominado «Identificación de documentación y legislación de referencia aplicable».

Asimismo, en lo que respecta a las entidades integrantes del sector público foral, corresponderá a cada una de ellas la identificación, mantenimiento y actualización de la normativa que les resulte de aplicación, lo cual deberá quedar debidamente documentado en su respectivo documento de «Identificación de documentación y legislación de referencia aplicable».

4. Principios de seguridad

El Consejo de Gobierno, de acuerdo con la Norma Foral 10/2023, de 15 de marzo, de gobierno, organización y régimen jurídico de la DFA, es el órgano colegiado de la Diputación Foral que bajo la dirección del Diputado General establece la política general, dirige la Administración Foral y ejerce las demás competencias que le atribuyen las Leyes y las Normas Forales y, a tal fin, ejerce la acción de gobierno, la iniciativa normativa, la potestad reglamentaria y la función ejecutiva.

La Política Corporativa de Protección de Datos Personales y de Seguridad de la Información de la Información será elaborada y definida por el Comité Corporativo de Seguridad y Privacidad, y será sometida a la aprobación del Consejo de Gobierno.

Como órgano colegiado director, se responsabilizará de la implantación de un modelo de seguridad que respete, como mínimo, los siguientes principios de seguridad:

D.L.: VI-1/1958 ISSN: 2254-8432

a) La seguridad de los sistemas de información será el resultado de un proceso integral dependiente de todos y cada uno de los elementos humanos, técnicos, materiales y organizativos que intervienen en su tratamiento.

b) Cada organización que desarrolle e implante sistemas de información realizará el correspondiente análisis y gestión de riesgos a los que están expuestos los mismos, monitorizando el nivel de exposición al riesgo, e implantando las posibles medidas tendentes a eliminarlo, disminuirlo o transferirlo. Las medidas de seguridad implementadas deberán estar actualizadas y deberán adaptarse a todas las fases del ciclo de vida de las aplicaciones y servicios relacionados con el tratamiento de la información, estableciendo un equilibrio entre la naturaleza de los datos, los tratamientos realizados, los riesgos expuestos y las medidas aplicadas. Para ello podrá recabar el asesoramiento de su Responsable de Seguridad y/o Delegado de Protección de Datos.

c) Todas las personas relacionadas con sistemas de información serán formadas e informadas de sus deberes y obligaciones en materia de seguridad, y se verificará que se siguen los procedimientos establecidos.

d) La seguridad de los sistemas de información estará atendida, revisada y auditada por personas cualificadas, dedicadas e instruidas en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

e) Los accesos a los sistemas de información serán controlados y limitados a las personas usuarias, procesos, dispositivos y otros sistemas de información debidamente autorizados, aplicándose criterios restrictivos a la hora de habilitar dichos accesos. Los sistemas de información serán diseñados y configurados de forma que garanticen la seguridad, proporcionando la mínima funcionalidad requerida para que la organización alcance sus objetivos.

f) Los sistemas de información se instalarán en áreas protegidas, dotadas de procedimientos de control de acceso físico.

g) Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. Se deberá conocer en todo momento su estado de seguridad, para lo que se tendrán en cuenta las especificaciones de los fabricantes, las vulnerabilidades que los afecten y las actualizaciones que las mitiguen o eliminen, reaccionando con diligencia para gestionar el riesgo correspondiente.

h) El uso de sistemas basados en Inteligencia Artificial (IA) en la Diputación Foral de Álava deberá realizarse de forma segura, responsable y alineada con los principios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información. La implantación y utilización de soluciones de IA estará sujeta a un análisis de riesgos específico y documentado, que deberá contemplar tanto los riesgos inherentes a la tecnología como los derivados de su interacción con otros sistemas y procesos de la organización. Se evaluará el impacto potencial sobre la seguridad de la información y la protección de los datos personales, asegurando el cumplimiento de la normativa vigente en materia de protección de datos y derechos digitales. En caso de que se trate de sistemas de inteligencia artificial de alto riesgo, se deberá llevar a cabo una evaluación de impacto relativa a los derechos fundamentales, de conformidad con el artículo 27 del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial.

D.L.: VI-1/1958 ISSN: 2254-8432

Además, se establecerán controles y salvaguardas para mitigar los riesgos identificados, incluyendo medidas para la gestión de sesgos, la transparencia en los procesos automatizados, la supervisión humana de los resultados y la trazabilidad de las decisiones automatizadas. Todo desarrollo, adquisición o despliegue de sistemas de IA deberá ser aprobado por la persona Responsable de Seguridad de Diputación Foral de Álava y estará sujeto a revisiones periódicas para garantizar su adecuación a los principios y requisitos de seguridad establecidos por la Diputación Foral de Álava.

i) La estructura y organización de la seguridad del sistema de información prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros, es decir, a la categoría de datos almacenados o al flujo de los mismos, así como a las deficiencias del entorno.

j) Los perímetros lógicos de la DFA se controlarán y protegerán del acceso de personas no autorizadas, en particular en las conexiones a las redes públicas. Se analizarán los riesgos derivados de la interconexión de los sistemas de información, a través de redes, con otros sistemas y se controlará su punto de unión.

k) La utilización de los sistemas podrá ser registrada, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas. Así mismo, aquellos procesos de gestión que requieran evidencias de su ejecución registrarán los datos necesarios para demostrar la existencia de los mismos, así como sus autoras/es.

l) Los sistemas de información dispondrán de medidas para la prevención, detección y reacción frente a código dañino (diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos), guardando especial cuidado en la instalación de los equipos para su tratamiento. Se incluirán además las medidas oportunas para su recuperación.

m) La detección de incidentes de seguridad o brechas de seguridad requerirá de una gestión de los mismos, de manera que tras su registro y resolución se puedan habilitar procesos de mejora continua de la seguridad de los sistemas.

n) Los sistemas de información dispondrán de copias de seguridad. Además, dispondrán de los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

o) Los sistemas de información deberán preservar la originalidad, legitimidad y consistencia de la información, así como la veracidad y autoría de la misma. De la misma manera, deberán registrar e identificar las acciones realizadas sobre los datos o aplicaciones.

p) Las auditorías validarán la aplicación efectiva de las políticas de seguridad, el cumplimiento de la legislación de aplicación en cada caso, así como la adecuación de las medidas de seguridad ante los riesgos identificados en las actividades de tratamiento.

q) La externalización de servicios será procedimentada con el fin de regular claramente el nivel de servicio de seguridad esperado y deberá suscribirse el correspondiente contrato de encargo de tratamiento cuando implique tratamiento de datos personales.

D.L.: VI-1/1958 ISSN: 2254-8432

r) La gestión de la seguridad a lo largo del ciclo de vida de desarrollo y adquisición de soluciones software se basará en metodologías reconocidas.

s) Los procesos de contratación relativos a sistemas de información deberán incluir referencia a que las empresas contratantes deberán estar homologadas o certificadas en seguridad de la información.

t) La gestión segura de los activos (sistemas de información) se establecerá regulando la clasificación de estos de acuerdo con su importancia y riesgo para los procesos de negocio, estableciendo los requerimientos que deben satisfacerse en su uso, e identificando a los responsables de los mismos. El nivel de protección y las medidas a aplicar se basarán en el resultado de dicha clasificación.

u) La gestión de los recursos humanos tendrá en cuenta requisitos de seguridad en los procedimientos selectivos, procesos de contratación, reorganización y cese.

v) La formación y concienciación en seguridad de la información serán componentes fundamentales para garantizar la protección efectiva de los sistemas. Se implementarán programas de formación en seguridad, adaptados a las necesidades de cada área, así como campañas de concienciación dirigidas a todo el personal, utilizando los medios más efectivos para asegurar la comprensión y cumplimiento de las políticas de seguridad.

w) Los sistemas de información dispondrán de un protocolo específico de actuación frente a ciberataques, en el que se incluirán además las condiciones de notificación al Centro Criptológico Nacional (CCN-CERT) que actúa como coordinador a nivel público estatal de las distintas capacidades de respuesta a incidentes de seguridad existentes.

x) La criptografía se empleará como un componente clave para garantizar la confidencialidad, integridad y autenticidad de la información en aquellos casos en que sea requerido. Se implementarán controles criptográficos conforme a la legislación vigente y en alineación con las mejores prácticas de seguridad.

y) Los datos personales serán tratados con el máximo rigor y en estricta conformidad con la normativa vigente en materia de protección de datos. Se implementarán medidas de seguridad adecuadas para garantizar la privacidad y protección de los datos personales, asegurando que su tratamiento sea limitado a los fines legítimos

El proceso integral de seguridad implantado será actualizado y mejorado de forma continua. Para ello será objeto de la oportuna gestión que garantice, a lo largo del tiempo, que se establezcan los controles y medidas para proteger los activos de la organización, y que se revisen y mejoren dichos controles y medidas para dar respuesta oportuna y proactivamente a las amenazas que vayan surgiendo, a los cambios regulatorios, o a las modificaciones en los objetivos de seguridad.

5. Objetivos

La implementación de los principios establecidos en la Política Corporativa de Protección de Datos Personales y de Seguridad de la Información posibilitará alcanzar objetivos a la DFA, garantizando así la seguridad integral de la información en todos los aspectos:

D.L.: VI-1/1958 ISSN: 2254-8432

a) Mantener unos niveles de seguridad óptimos en términos de Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad, ajustados y coherentes con las necesidades de la DFA y de la ciudadanía.

b) Garantizar el cumplimiento del marco legal vigente.

c) Promover una cultura de ciberseguridad entre el personal de la DFA.

d) Mantener un Sistema de Gestión de la Seguridad y Privacidad de la Información para identificar, analizar y tratar los riesgos asociados a los activos, servicios y procesos de la DFA.

e) Implantar medidas técnicas y organizativas que proporcionen el nivel de seguridad adecuado, con alcance a los sistemas y procesos que tratan esta información.

f) Implantar mecanismos de contingencia para permitir la continuidad de los servicios y sistemas de información, permitiendo la recuperación de los mismos en un periodo aceptable.

6. Organización

La DFA dispondrá de una estructura organizativa para la gestión y coordinación de la Seguridad y Protección de Datos Personales, con una identificación de las responsabilidades derivadas de la presente Política Corporativa en sus aspectos de definición, implantación, operación, gestión, seguimiento y comunicación. Dicha Organización de la Seguridad y Privacidad de la Información se responsabilizará de:

a) Establecer los mecanismos necesarios para responder eficazmente a los incidentes de seguridad.

Ejecutar los procesos de seguridad de acuerdo a los roles de seguridad establecidos.

b) Definir, implantar, gestionar y supervisar los controles organizativos, y técnicos específicos para mantener la seguridad de los activos accedidos por terceras partes y en los casos en que la responsabilidad del procesamiento de la información haya sido delegada en otra organización.

c) Establecer los mecanismos apropiados para la cooperación en materia de seguridad con las autoridades competentes, empresas proveedoras de servicios, así como organismos públicos o privados dedicados a promover la seguridad de los sistemas de información.

La Organización se adecuará a la estructura funcional de cada Organización, contemplará tanto roles de carácter multipersonal como unipersonal, y tendrá en cuenta el nivel funcional de los mismos (estratégico, táctico, operativo y de control), tanto para los entornos de negocio (clientes del servicio de seguridad), como para los de soporte (empresas proveedoras del servicio de seguridad), y se implantará de acuerdo a los siguientes principios:

a) Se establecerá una Organización de Seguridad para todo el ámbito de la DFA, considerando la misma con un carácter de mínimos, y facultando la creación, en entornos concretos de la DFA, de organizaciones de seguridad complementarias a la establecida con carácter general, siempre que dichas organizaciones respeten y superen el carácter de mínimos del modelo organizativo global.

D.L.: VI-1/1958 ISSN: 2254-8432

b) Integrará en el modelo de organización global aquellas iniciativas organizativas actualmente implantadas, y facilitará la coordinación entre las distintas iniciativas particulares adoptadas en entornos concretos de la DFA mediante su alineamiento e integración en el modelo organizativo global.

c) Cualquier modificación del organigrama interno que conlleve la supresión o modificación de alguno de los puestos vinculados a la aplicación del ENS, tendrá que incorporar obligatoriamente el puesto al que quedarán vinculadas esas funciones.

d) Será adaptable a cada uno de los dominios técnicos u organizativos en los que dicha organización tenga responsabilidades.

e) Los roles y responsabilidades adheridos a la presente Política formarán parte de la estructura organizativa de la DFA y deberán ser adaptados a cada uno de los órganos administrativos de la Diputación, así como al Sector Público Foral. El detalle de los roles, funciones y responsabilidades de cada rol se encuentran descritos en el documento Organización de Seguridad y Protección de Datos.

7. Desarrollo del Cuerpo Documental Protección de Datos Personales y de Seguridad de la Información

La estructura del Cuerpo Documental Protección de Datos Personales y de Seguridad de la Información se organiza mediante la definición inicial de la presente política, de la cual emanarán una serie de **normas** (que detallarán los objetivos a alcanzar en relación a uno o varios de los aspectos concretos de la presente Política), **procedimientos** (que recogerán el conjunto de tareas detalladas, secuenciales y específicas con el fin de soportar, en la operativa diaria, todos los procesos de seguridad), **metodologías**, **directrices**, **buenas prácticas**, etc., en los cuales se definirán las distintas medidas a tomar para proteger el sistema de información, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar su correcto funcionamiento.

Los diversos componentes del Cuerpo Documental serán redactados, revisados y aprobados por aquellas/os integrantes de la Organización de Seguridad y Privacidad de la Información que correspondan al carácter estratégico, táctico u operativo de dichos componentes, estableciéndose para ello el correspondiente procedimiento que regule su ciclo de vida.

8. Actualización y revisión de la Política Corporativa de Protección de Datos Personales y de Seguridad de la Información

Siendo la permanencia e integridad de la Política Corporativa de Protección de Datos Personales y de Seguridad de la Información uno de los requisitos fundamentales que la misma debe cumplir con el fin de que constituya un marco de actuación de carácter estable que permita desarrollar el Cuerpo Documental, será necesaria su actualización con el fin de que la misma no pierda su efectividad y adecuación.

Por ello, la Política Corporativa de Protección de Datos Personales y de Seguridad de la Información será objeto de una revisión periódica bienal, siempre y cuando no existan cambios significativos (nueva legislación, nuevas amenazas o riesgos, cambios estratégicos que afecten a los sistemas de información…), o que de las conclusiones obtenidas de los procesos de revisión de la seguridad se imponga la necesidad de proceder a su revisión, modificación y perfeccionamiento inmediato.

D.L.: VI-1/1958 ISSN: 2254-8432

La recomendación de estabilidad durante el periodo de vigencia de la Política Corporativa de Protección de Datos Personales y de Seguridad de la Información (que marca las directrices corporativas) no afecta al Cuerpo Documental, ya que éste debe ser revisado y actualizado con la frecuencia necesaria para adaptarse a los cambios técnicos de la infraestructura y a los requisitos del negocio. En el caso de que algún apartado del Cuerpo Documental presente incongruencia alguna con la presente Política Corporativa de Protección de Datos Personales y de Seguridad de la Información, ésta tendrá prioridad.

La Política Corporativa de Protección de Datos Personales y de Seguridad de la Información estará publicada en el BOTHA, así como en la Intranet de los órganos administrativos, sociedades y organismos en los que sea de aplicación.

9. Incumplimiento de la Política Corporativa de Protección de Datos Personales y de Seguridad de la Información

El Comité Corporativo de Seguridad y Privacidad podrá apreciar si por parte del personal que tiene acceso a la información de la DFA, o trata dicha información en el ejercicio de sus actividades profesionales, existe algún tipo de incumplimiento de las obligaciones previstas en la Política Corporativa de Protección de Datos Personales y de Seguridad de la Información o en su normativa interna.

En caso de incumplimiento, se prevén medidas preventivas y correctivas encaminadas a salvaguardar y proteger la información, sin perjuicio del régimen sancionador aplicable en el ejercicio de los Altos cargos de Diputación Foral de Álava (capítulo VI de la Norma Foral 10/2018, de 11 de julio") así como en lo relativo a la actuación de las personas funcionarias (Ley 11/2022, de 1 de diciembre, de Empleo Público Vasco. Título XII).

10. Aprobación y entrada en vigor

La Política Corporativa de Protección de Datos Personales y de Seguridad de la Información será aplicable al día siguiente de la publicación en el BOTHA y hasta que sea reemplazada por una nueva versión.

D.L.: VI-1/1958 ISSN: 2254-8432

Arabako Foru Aldundia
Diputación Foral de Álava

DOSORGSG – ORGANIZACIÓN DE SEGURIDAD Y PROTECCIÓN DE DATOS

Clasificación del documento: Público

Organización de la Seguridad y Protección de Datos
Clasificación del documento: Público

D.L.: VI-1/1958 ISSN: 2254-8432

Hoja de control:

Documento:	
Autor:	
Versión:	**Fecha de versión:**
Revisado por:	**Fecha de revisión:**
Aprobado por:	**Fecha de aprobación:**

Control de cambios:

Versión	Fecha	Elaborado por:	Descripción

Organización de la Seguridad y Protección de Datos
Clasificación del documento: Público

D.L.: VI-1/1958 ISSN: 2254-8432

D.L.: VI-1/1958 ISSN: 2254-8432

Arabako Foru Aldundia
Diputación Foral de Álava

1. Introducción

1.1. Objetivos

Establecer una estructura organizativa de la Diputación Foral de Álava (en adelante, DFA) que garantice un gobierno, operación, supervisión y control efectivo de sus actividades. Esto incluye la definición detallada de roles y responsabilidades relacionados con la Seguridad de la Información, y protección de los datos abarcando su desarrollo, implementación, gestión y mantenimiento para asegurar un enfoque integral y proactivo en la protección de los activos de la DFA.

La estructura y los roles definidos en este documento están diseñados para implementar y alinearse plenamente con los principios establecidos en la Política Corporativa de Seguridad de la Información de DFA, promoviendo una cultura organizacional comprometida con la Seguridad de la Información.

1.2. Alcance

El modelo de Organización de Seguridad descrito se aplica a toda la DFA y sus personas usuarias, tanto internas como externas. La protección de la Seguridad de la Información y la protección de los datos es una responsabilidad compartida y no recae únicamente en aquellas que, por razón de su cargo o funciones, tienen asignadas responsabilidades específicas en el desarrollo y gestión de la seguridad de los sistemas de información.

2. Roles de Seguridad

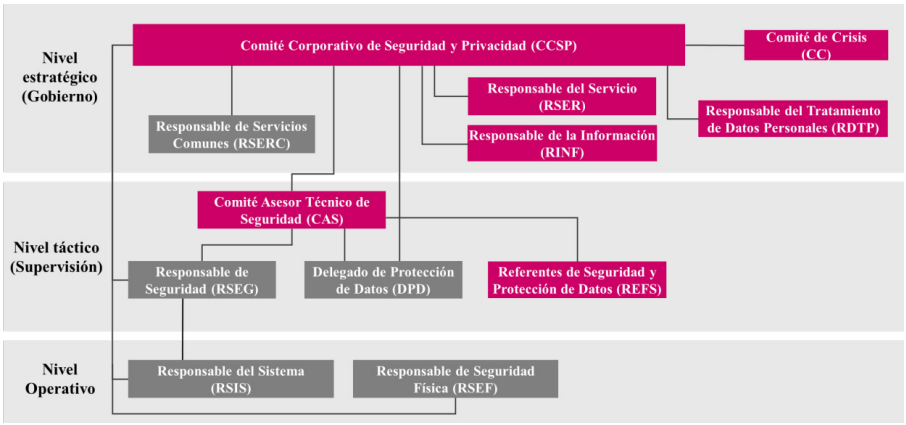
2.1. Visión general de Roles de Seguridad

En el contexto de la Seguridad de la Información, establecer una estructura clara y efectiva de roles es fundamental para la protección de la información y los sistemas de la DFA. Esta sección ofrece una visión general de los roles de seguridad, destacando sus responsabilidades y funciones dentro de la DFA. Cada rol está vinculado a un nivel específico de seguridad, asegurando que las medidas de protección sean adecuadas y proporcionales a las necesidades y riesgos asociados a cada función dentro de la DFA. Además, es necesario considerar la normativa del RGPD, que establece normas de obligado cumplimiento sobre la gestión y protección de datos personales, garantizando que las prácticas de seguridad de la DFA cumplan con los estándares legales europeos y protejan la protección de los individuos involucrados. Este enfoque es coherente con la Directiva NIS2, que exige una definición clara de roles y responsabilidades en materia de ciberseguridad para una gestión eficaz de los riesgos.

En el presente modelo de Organización de Seguridad de la DFA, se han definido tres capas diferenciadas enfocadas específicamente en la Protección de Datos y Sistemas de Información: Gobierno, Supervisión y Operación. La capa de Gobierno establece las políticas y directrices estratégicas; la capa de Supervisión se encarga de asegurar la monitorización constante y el cumplimiento de las políticas y directrices de seguridad; la capa de Operación se centra en la implementación de las medidas de seguridad necesarias.

De manera gráfica, se presenta el mapa de roles de seguridad, que recoge de forma estructurada los diversos roles implicados en la gestión de la Seguridad de la Información, organizados en base a las capas previamente definidas:

D.L.: VI-1/1958 ISSN: 2254-8432



Los roles multipersonales se representan en cajas de color rojo, mientras que los roles unipersonales se representan en cajas de color gris. Esta distinción es crucial para asegurar que los roles de seguridad se integren adecuadamente en la estructura organizativa de la DFA, en cada una de sus Direcciones. La asignación de roles multipersonales se concretará especificando a sus integrantes, mientras que los roles unipersonales se designarán según los niveles jerárquicos apropiados dentro de la estructura organizativa.

2.2. Descripción de Roles de Seguridad

En los siguientes apartados, se recoge la descripción de los roles anteriormente identificados. Dichos roles están alineados con las directrices que al respecto se establecen en la Política Corporativa de Seguridad de la Información.

2.2.1. Comité Corporativo de Seguridad y Privacidad (CCSP)

El Comité Corporativo de Seguridad y Privacidad (CCSP) desempeña un papel crucial en la protección de los activos de la DFA. Es responsable de coordinar y supervisar las iniciativas de seguridad, asegurando que se alineen con los objetivos corporativos y cumplan con las normativas aplicables. El Comité se reunirá con una periodicidad **mínima anual**.

2.2.1.1. Funciones generales del Comité Corporativo de Seguridad y Privacidad

Las funciones del Comité Corporativo de Seguridad y Privacidad (CCSP) serán las siguientes:

- Definir los objetivos de la DFA en materia de Seguridad de la Información y asegurar que los mismos están en conexión con los requisitos de negocio, los procesos más relevantes, y las normativas que le afecten.

D.L.: VI-1/1958 ISSN: 2254-8432

- Aprobar la Política Corporativa de Seguridad de la Información.
- Aprobar la estrategia de seguridad y los planes de mejora propuestos por el Responsable de Seguridad, asegurando su alineación con los objetivos generales de la DFA.
- Aprobar las obligaciones y funciones que se establezcan dentro la DFA en materia de Seguridad de la Información, así como resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre las diferentes áreas de la DFA
- Aprobar el umbral del riesgo corporativo, estableciendo el marco de tolerancia al riesgo que guíe la toma de decisiones sobre la aceptación y tratamiento de los riesgos identificados en la organización
- Ser informado periódicamente del estado de la Seguridad de la Información de la DFA, incluyendo riesgos relevantes, incidentes significativos y grado de cumplimiento normativo.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información, mediante la aprobación de planes específicos, incluidos los relativos a resiliencia y continuidad operativa conforme a NIS2
- Supervisar y coordinar la asignación y gestión eficiente de los recursos financieros, tecnológicos y humanos destinados a la Seguridad de la Información, asegurando que el presupuesto asignado sea acorde con las necesidades estratégicas y operativas, y priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados, con el fin de garantizar la adecuada implementación, mantenimiento y mejora continua de las medidas de seguridad.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Supervisar la gestión de los incidentes de Seguridad de la Información, recibir información de los incidentes relevantes y, en su caso, adoptar decisiones estratégicas y priorizar recursos.
- Velar porque se respete el principio de seguridad en todas aquellas iniciativas de la entidad que afecten a la Seguridad, promoviendo la adopción de servicios horizontales y soluciones comunes que reduzcan duplicidades, garanticen un funcionamiento homogéneo de los sistemas en el ámbito del ENS y faciliten el cumplimiento del resto de normativas aplicables.
- Impulsar y aprobar planes de formación, concienciación y cultura de seguridad en la DFA.

El Comité se reunirá con una periodicidad **mínima anual**, con el objeto de aprobar la gestión de la Seguridad de la Información realizada en el ejercicio anterior y establecer las líneas estratégicas y prioridades en esta materia para el ejercicio siguiente.

Asimismo, podrá reunirse de forma extraordinaria ante incidentes relevantes o situaciones excepcionales que, por su impacto o trascendencia, requieran la adopción de decisiones estratégicas o la priorización de recursos, a juicio de la Presidencia o a propuesta del Responsable de Seguridad.

La Presidencia del Comité Corporativo de Seguridad y Privacidad recaerá en la persona titular de la Dirección de Servicios Generales de la DFA, o en la persona en quien delegue.

El Responsable de Seguridad de la DFA actuará como Secretario del Comité, con las siguientes funciones:

- Convocar las reuniones del Comité Corporativo de Seguridad y Privacidad (CCSP), por instrucción de la Presidencia.
- Preparar los asuntos a tratar, recabando la información necesaria de los distintos responsables.
- Elaborar las actas de las reuniones.
- Remitir el acta de las reuniones a los asistentes, recabando su firma
- Custodiar las actas conforme a los criterios de conservación documental de la entidad.

2.2.1.2. Integrantes del Comité Corporativo de Seguridad y Privacidad

El Comité Corporativo de Seguridad y Privacidad estará formado por todas aquellas personas que participen en la responsabilidad, definición o implantación de la Seguridad de la Información tratada o los servicios prestados:

- Consejo de Gobierno.
- La persona titular de la Dirección de Servicios Generales, que ejercerá la Presidencia.
- El Responsable de Seguridad (RSEG) de la DFA, que actuará como Secretario.
- Responsable de Seguridad TIC (RSTIC-CCASA) de CCASA.
- Responsable de Servicios Comunes (RSERC).
- Responsable de Seguridad Física (RSEF).
- Responsable del Sistema (RSIS).

Participarán con carácter asesor:

- El Delegado de Protección de Datos (DPD), de conformidad con lo dispuesto en el RGPD.

Asimismo:

- Podrán participar, como personas invitadas, aquellas que se consideren necesarias en función de los asuntos a tratar.

2.2.2. Comité de Crisis (CC)

El Comité de Crisis (CC) se convocará a **demanda**, ante la aparición de incidentes o situaciones que requieran su intervención inmediata para la activación de protocolos, toma de decisiones urgentes, y la activación formal de protocolos de crisis.

2.2.2.1. Funciones generales del Comité de Crisis

Las funciones del Comité de Crisis (CC) serán las siguientes:

- Activar los protocolos de contingencia y continuidad para hacer frente a situaciones excepcionales que puedan afectar el normal funcionamiento de la DFA.
- Aprobar medidas operativas excepcionales que permitan una respuesta eficaz y proporcional a la gravedad e impacto de la crisis.
- Coordinar, cuando resulte necesario, la notificación a los organismos y autoridades competentes, conforme a la normativa aplicable (ENS, NIS2 y RGPD)
- Supervisar las acciones de recuperación y mitigación del impacto derivado de la crisis, asegurando la rápida restauración de los servicios esenciales y minimizando pérdidas.
- Evaluar y decidir sobre la activación y desactivación del Comité de Crisis, en función de la evolución de la situación.
- Mantener informado al Comité Corporativo de Seguridad y Privacidad y a otros órganos decisores sobre la evolución de la crisis, los riesgos identificados y las medidas adoptadas.
- Garantizar la coordinación entre las diferentes áreas implicadas, facilitando la comunicación y colaboración interdepartamental.
- Promover la revisión posterior a la crisis, con el fin de identificar lecciones aprendidas y mejorar los planes de contingencia y resiliencia.

Otras funciones que se asignen al Comité de Crisis, relacionadas con la gestión de situaciones excepcionales, deberán ser aprobadas por el Comité Corporativo de Seguridad y Privacidad.

D.L.: VI-1/1958 ISSN: 2254-8432

La Presidencia del Comité de Crisis recaerá en la persona Responsable de la Seguridad (RSEG), o en la persona en quien delegue.

2.2.2.2. Integrantes del Comité de Crisis

El Comité de Crisis estará formado por las personas que desempeñen roles clave en la coordinación, ejecución y supervisión de las medidas de respuesta a incidentes críticos, entre ellas:

- Diputado/a responsable de Dirección de Servicios Generales de DFA y CCASA.
- Director/a Gerente de CCASA.
- Responsable de Seguridad de DFA (RSEG).
- Responsable de Seguridad TIC de CCASA.
- Responsable del Sistema (RSIS).
- Responsable del Área de Infraestructuras de CCASA.
- Dirección a cargo de la Jefatura del Servicio de Asesoría Jurídica de DFA.
- Dirección de Gabinete y Comunicación.
- Delegado/a de Protección de Datos (DPD), cuando el incidente afecte a datos personales.

2.2.3. Comité Asesor Técnico de Seguridad (CAS)

El Comité Asesor Técnico de Seguridad (CAS) es el órgano de carácter técnico encargado de analizar, elaborar y proponer las medidas técnicas y organizativas necesarias para la implantación, seguimiento y mejora de la Seguridad de la Información en la DFA. Desempeña sus funciones en coordinación con los distintos roles y órganos definidos en el modelo de gobierno de la seguridad, garantizando el cumplimiento de la normativa aplicable y la adecuada alineación de las medidas propuestas con los objetivos corporativos establecidos por el Comité Corporativo de Seguridad y Privacidad.

El Comité se reunirá con una periodicidad **semestral.**

2.2.3.1. Funciones generales del Comité Asesor Técnico de Seguridad

Las funciones del Comité Asesor Técnico de Seguridad (CAS) serán las siguientes:

- Coordinar técnicamente la aplicación de las medidas y controles definidos.
- Elaborar propuestas técnicas y borradores relativos a la evolución de la seguridad, adaptados a los cambios tecnológicos, normativos y de riesgo

D.L.: VI-1/1958 ISSN: 2254-8432

- Proponer la categoría de los sistemas de información.
- Elaborar el borrador técnico para la Declaración de Aplicabilidad.
- Preparar informes técnicos sobre incidentes, auditorías, controles y planes de auditoría, formación y continuidad, para su elevación al Responsable de Seguridad
- Ejecutar y coordinar técnicamente el análisis y la gestión de riesgos, así como los BIAs y planes de continuidad de negocio.
- Tratar los conflictos de carácter técnico relacionados con la seguridad y elevarlos al Responsable de Seguridad y, cuando proceda, al Comité Corporativo de Seguridad y Privacidad (CCSP).
- Aportar criterios y recomendaciones técnicas que faciliten la adecuada implementación de los requisitos legales y normativos en materia de seguridad y protección de datos personales.
- Evaluar nuevas tecnologías y riesgos emergentes que puedan afectar a la seguridad, proponiendo las medidas necesarias para su adecuada gestión.
- Prestar soporte técnico en la implantación de medidas derivadas de la normativa de protección de datos personales, en coordinación con la persona Delegada de Protección de Datos y los responsables del Tratamiento.

Otras funciones de carácter técnico que se asignen al Comité Asesor Técnico de Seguridad deberán ser aprobadas por el Comité Corporativo de Seguridad y Privacidad, especialmente aquellas relacionadas con la gestión de la seguridad a nivel técnico.

La presidencia del Comité Asesor Técnico de Seguridad recaerá en la persona Responsable de Seguridad, o en la persona en quien delegue.

2.2.3.2. Integrantes del Comité Asesor Técnico de Seguridad

El Comité Asesor Técnico de Seguridad estará formado por las personas que desempeñen roles clave en la gestión técnica y coordinación de la seguridad de la información dentro de la entidad, entre ellas:

- Responsable de Seguridad (RSEG).
- Referentes de Seguridad (REFS).
- Responsable de Seguridad TIC de CCASA.
- Personal técnico de CCASA, en función de las materias a tratar.

Participarán con carácter asesor:

- Delegado/a de Protección de Datos (DPD), cuando los asuntos tratados estén relacionados con la protección de datos personales.
- Personas asesoras externas, que podrán participar a demanda, en función de las necesidades específicas de la entidad o de los asuntos a tratar

2.2.4. Responsable de Seguridad (RSEG)

El Responsable de Seguridad (RSEG) es responsable de determinar las decisiones necesarias para satisfacer los requisitos de Seguridad de la Información y de los servicios de la DFA, asegurando la coherencia, adecuación y eficacia del sistema de seguridad.

Para ello, supervisa la implantación y ejecución de las medidas técnicas y organizativas, y actúa como enlace entre los órganos de gobierno, los responsables funcionales y los equipos técnicos, con el fin de garantizar el cumplimiento de los requisitos establecidos de conformidad con la normativa aplicable.

2.2.4.1. Funciones Generales del Responsable de Seguridad

Las funciones del Responsable de Seguridad serán las siguientes:

- Determinar y supervisar las decisiones necesarias para garantizar el cumplimiento de los requisitos de Seguridad de la Información y de los servicios de la DFA, asegurando la coherencia, adecuación y eficacia del sistema de seguridad
- Convocar y coordinar el funcionamiento del Comité Corporativo de Seguridad y Privacidad (CCSP), actuando como órgano técnico de apoyo y elevando para su revisión o aprobación las políticas, normativas, planes e informes en materia de Seguridad de la Información.
- Proponer al CCSP la Política Corporativa de Seguridad de la Información, la normativa de seguridad y el Plan de Mejora de la Seguridad, incluyendo la correspondiente propuesta de dotación de recursos.
- Actuar como canal de enlace y comunicación con el CCSP en relación con los incidentes relevantes de seguridad, los riesgos significativos y las directrices estratégicas en materia de seguridad de la información.
- Aprobar la Declaración de Aplicabilidad del Esquema Nacional de Seguridad, elaborada por los órganos técnicos competentes
- Validar el marco normativo de seguridad de la información —políticas, normas, procedimientos, instrucciones y guías— elaborado por los órganos técnicos competentes, asegurando su adecuación al Esquema Nacional de Seguridad (ENS), a la Directiva NIS2 y al resto de la normativa vigente que resulte de aplicación.

- Coordinar y supervisar la realización de los análisis de riesgos de los sistemas de información, validando la categoría de los sistemas a partir de las valoraciones realizadas por los Responsables de la Información (RINF) y de los Servicios (RSER).

- Revisar y validar los riesgos residuales aceptados por los responsables correspondientes, comprobando su adecuación al umbral de riesgo corporativo aprobado por la organización.

- Elevar al órgano competente los informes consolidados sobre el nivel de riesgo global de la DFA.

- Velar por la incorporación de los principios y obligaciones del Reglamento General de Protección de Datos y de los requisitos normativos aplicables a sistemas basados en inteligencia artificial en el diseño e implantación de las medidas técnicas y organizativas, en coordinación con el Delegado/a de Protección de Datos y las figuras responsables.

- Realizar el seguimiento permanente de la legislación nacional e internacional en materia de Seguridad de la Información, protección de datos personales y regulación aplicable a tecnologías emergentes, incluidos los sistemas basados en inteligencia artificial, promoviendo su correcta interpretación, aplicación y cumplimiento en la DFA.

- Analizar y validar los riesgos de seguridad asociados al uso de sistemas basados en inteligencia artificial, con carácter previo y posterior a su despliegue.

- Supervisar el estado de la seguridad de los sistemas, a partir de los informes y evidencias facilitadas por los responsables técnicos y los proveedores de servicios.

- Definir los criterios e indicadores de seguimiento de la seguridad y validar los informes de métricas correspondientes.

- Supervisar el cumplimiento de las obligaciones en materia de seguridad por parte de los proveedores de servicios externalizados.

- Coordinar la gestión de los incidentes de Seguridad de la Información, elevando la información al Comité de Crisis o al CCSP cuando proceda.

- Ejercer las funciones que le correspondan en materia de continuidad del negocio y recuperación ante desastres, de conformidad con el marco de continuidad aprobado.

- Actuar como punto de contacto de la DFA ante autoridades competentes, organismos y agentes externos en materia de Seguridad de la Información.

D.L.: VI-1/1958 ISSN: 2254-8432

2.2.5. Responsable del Tratamiento de Datos Personales (RTDP)

Serán responsables del Tratamiento de datos personales las personas titulares de las Direcciones bajo cuya responsabilidad se realicen los correspondientes tratamientos, de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y la normativa aplicable.

2.2.5.1. Funciones Generales del Responsable del Tratamiento de datos personales

Las funciones del Responsable del tratamiento serán las siguientes:

- Determinar y aplicar las medidas técnicas y organizativas de seguridad adecuadas a los tratamientos de datos que se encuentren bajo su responsabilidad.
- Impulsar y asegurar la realización, cuando proceda, de los análisis de riesgos y de las evaluaciones de impacto en materia de protección de datos, en coordinación con de la persona delegada de protección de datos y los órganos técnicos competentes.
- Garantizar la notificación de las brechas de seguridad de los datos personales a la autoridad de control competente y, en su caso, a las personas interesadas, dentro de los plazos legalmente establecidos, contando para ello con el asesoramiento de la persona Delegada de Protección de Datos y la coordinación del Responsable de Seguridad.
- Resolver las solicitudes de ejercicio de derechos en materia de protección de datos personales (artículos 15 a 22 del RGPD), con el apoyo de las unidades responsables y el asesoramiento de la persona Delegada de Protección de Datos.
- Desempeñar el resto de funciones que le atribuya la normativa vigente en materia de protección de datos personales.

2.2.6. Responsable de la Información (RINF)

La figura del Responsable de Información será asumida por una persona designada de cada Dirección, a la que corresponderá la responsabilidad última sobre el uso, protección y adecuación de la información bajo su ámbito competencial.

Las responsabilidades del RINF podrían ser unificadas con las responsabilidades del Responsable del Servicio (RSER, descritas en el apartado 2.2.7).

El Responsable de la Información ejercerá sus funciones con el apoyo de las personas Referentes de Seguridad y de las unidades técnicas correspondientes.

2.2.6.1. Funciones Generales del Responsable de la Información

Las funciones del Responsable de Información serán las siguientes:

- Establecer los requisitos de seguridad de la información bajo su responsabilidad, asegurando que se establecen los niveles de protección necesarios para garantizar su confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y protección

D.L.: VI-1/1958 ISSN: 2254-8432

de datos, de conformidad con los principios y requisitos estipulados en las políticas y normas de DFA, así como con la legislación aplicable con el Esquema Nacional de Seguridad y la normativa aplicable.

- Participar activamente en los procesos de análisis y categorización de riesgos asociados a la información, colaborando con los órganos responsables para identificar, evaluar y clasificar las vulnerabilidades y amenazas, a fin de definir las medidas de protección adecuadas conforme a la normativa y políticas vigentes.

- Asumir y aceptar los riesgos residuales derivados de la gestión de la información bajo su responsabilidad, siempre que estos se encuentren dentro de los umbrales de riesgo corporativos aprobados por la organización.

- Comunicar de manera oportuna y precisa el impacto de los incidentes de seguridad que afecten a la información.

2.2.7. Responsable del Servicio (RSER)

La figura del Responsable del Servicio (RSER) será asumida por una persona designada de cada Dirección a la que corresponderá la responsabilidad última sobre la prestación, disponibilidad y adecuación de los servicios bajo su ámbito competencial.

Las responsabilidades del RSER podrían ser unificadas con las responsabilidades del Responsable de la Información (RINF, descritas en el apartado 2.2.6).

2.2.7.1. Funciones Generales del Responsable del Servicio

Las funciones del Responsable de Servicio serán las siguientes:

- Definir los requisitos de seguridad y disponibilidad de los servicios bajo su responsabilidad, estableciendo los niveles necesarios para garantizar su correcta prestación, de conformidad con las políticas y normas de la DFA y el Esquema Nacional de Seguridad.

- Identificar y determinar los servicios críticos desde el punto de vista de su impacto en la actividad de la organización, aportando esta información a los procesos de análisis de riesgos y continuidad.

- Participar en los análisis de riesgos y en los Análisis de Impacto en el Negocio (BIA) y el Plan de Continuidad de Negocio asociados a los servicios, colaborando con los órganos técnicos competentes para la identificación de amenazas, vulnerabilidades e impactos.

- Asumir y aceptar los riesgos residuales asociados a los servicios bajo su responsabilidad, siempre que se mantengan dentro de los umbrales de riesgo corporativos aprobados.

D.L.: VI-1/1958 ISSN: 2254-8432

- Comunicar de forma adecuada el impacto de los incidentes de seguridad que afecten a los servicios, facilitando su gestión por los órganos responsables

2.2.8. Responsable de servicios comunes (RSERC)

La figura del Responsable de Servicios Comunes (RSERC) será asumido por la persona designada al efecto, a la que corresponderá la responsabilidad de coordinar y definir los requisitos de seguridad aplicables a los servicios de carácter común y compartido en la DFA, con el fin de garantizar un enfoque homogéneo, coherente y eficiente.

El Responsable de Servicios Comunes (RSERC) ejercerá sus funciones en coordinación con el Responsable de Seguridad, los responsables de los servicios afectados y los órganos técnicos competentes.

2.2.8.1. Funciones Generales del Responsable de Servicios Comunes

Las funciones Responsable de Servicios Comunes serán las siguientes:

- Garantizar la coordinación entre los distintos responsables de servicios, con el fin de asegurar la coherencia, estandarización y adecuación de las medidas de seguridad aplicadas a los servicios comunes y compartidos

- Evaluar las necesidades estratégicas y operativas de seguridad de los servicios comunes, considerando su evolución tecnológica, los cambios normativos y los requisitos derivados de la actividad de la organización

- Participar en la definición de los modelos de gobernanza y control asociados a la seguridad de la infraestructura compartida y de los servicios comunes.

- Coordinar y supervisar el cumplimiento de los requisitos de seguridad por parte de los proveedores y terceros involucrados en los servicios comunes, de acuerdo con lo establecido en los acuerdos contractuales y la normativa aplicable, en coordinación con el Responsable de Seguridad.

- Impulsar la mejora continua de la seguridad de los servicios comunes, mediante la propuesta de planes, proyectos y actuaciones orientadas a la reducción del riesgo y la optimización de las capacidades de protección.

- Colaborar con los distintos órganos y áreas de la organización para asegurar la alineación de la seguridad de los servicios comunes con la estrategia global de Seguridad de la Información definida por el Comité Corporativo de Seguridad y Privacidad

2.2.9. Delegado de Protección de Datos (DPD)

La figura Delegada de Protección de Datos es la persona designada para informar, asesorar y supervisar el cumplimiento de la normativa en materia de protección de datos personales en la DFA, conforme a lo dispuesto en el Reglamento General de Protección de Datos.

La persona Delegada de Protección de Datos ejercerá sus funciones con plena independencia, sin recibir instrucciones en lo que respecta al ejercicio de sus cometidos, y actuará como órgano asesor y de supervisión, sin asumir responsabilidades operativas en la gestión de los tratamientos.

2.3. Funciones Generales del Delegado/a de Protección de Datos

Las funciones del Delegado/a de Protección de Datos serán las siguientes:

- Informar y asesorar al responsable y al encargado del tratamiento, así como al personal que participe en las operaciones de tratamiento, sobre las obligaciones que les incumben en virtud del Reglamento General de Protección de Datos y del resto de normativa aplicable en materia de protección de datos personales

- Supervisar el cumplimiento de lo dispuesto en el Reglamento General de Protección de Datos, de las políticas internas de la DFA en materia de protección de datos personales y de la correcta asignación de responsabilidades, incluyendo las acciones de concienciación y formación

- Asesorar al responsable del tratamiento cuando se le solicite en relación con la realización de evaluaciones de impacto relativas a la protección de datos y supervisar su correcta aplicación.

- Asesorar al responsable del tratamiento en la gestión de las brechas de seguridad de los datos personales, incluyendo la notificación a la autoridad de control y, en su caso, a las personas interesadas, conforme a los plazos y requisitos establecidos en el Reglamento General de Protección de Datos.

- Cooperar con la autoridad de control y actuar como punto de contacto de la misma para cuestiones relativas al tratamiento, incluida la consulta previa y otras actuaciones que procedan

- Participar con carácter asesor en comités, grupos de trabajo y otros órganos de gobernanza en los que se traten cuestiones relacionadas con la protección de datos personales, aportando criterios especializados para garantizar el cumplimiento normativo.

- Realizar el seguimiento de la normativa vigente en materia de protección de datos personales, tanto a nivel nacional como internacional, informando de los cambios relevantes que puedan afectar a la actividad de la DFA.

- Asesorar y supervisar la elaboración, revisión y actualización de las políticas internas en materia de protección de datos personales, verificando su alineación con la normativa aplicable.

2.4. Referentes de Seguridad y Protección de Datos (REFS)

La figura del Referente de Seguridad será desempeñada por las Jefaturas de Servicio y/o personas en las que deleguen, actuando como punto de apoyo operativo y de enlace en materia de Seguridad de la Información y Protección de Datos dentro de su ámbito organizativo.

Su función es facilitar la correcta aplicación de las medidas establecidas, actuando como enlace con los responsables corporativos en actividades de análisis de riesgos, análisis de Impacto en el Negocio (BIA), planes de continuidad, auditorías y planes de mejora, así como en el apoyo al Responsable del Tratamiento en el cumplimiento de la normativa de protección de datos personales. En este sentido, participarán en la identificación y gestión de riesgos, la realización de evaluaciones de impacto cuando proceda, la gestión de brechas de seguridad y la adecuada implantación de medidas técnicas y organizativas.

El modelo organizativo permite que una misma persona pueda asumir distintos roles, lo que requiere una coordinación continua entre los diferentes responsables, así como la adecuada dotación de medios y recursos técnicos que garanticen el cumplimiento efectivo de las obligaciones establecidas.

2.4.1.1. Funciones Generales del Referente de Seguridad y Protección de Datos

Las funciones del Referente de Seguridad y Protección de Datos serán las siguientes:

- Colaborar y facilitar la realización de auditorías de seguridad en su ámbito, así como el seguimiento operativo de los planes de mejora derivados de las mismas.
- Ejercer funciones de interlocución entre su departamento o entidad y los responsables corporativos de seguridad (RINF y RSER), facilitando la comunicación efectiva y fluida.
- Impulsar, coordinar y colaborar en la difusión y correcta aplicación de las medidas técnicas y organizativas en materia de Seguridad de la Información dentro de su ámbito.
- Participar activamente en los procesos de análisis de riesgos, Análisis de Impacto en el Negocio (BIA) y en la elaboración y seguimiento de los planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP), aportando información y conocimiento del servicio.
- Elaborar y facilitar la información, evidencias y documentación requerida en materia de Seguridad de la Información relativa a su departamento o entidad
- Informar de manera periódica y sistemática sobre el estado de la seguridad de la información, los riesgos identificados y las incidencias detectadas en su ámbito a los responsables corporativos (RINF y RSER).

- Apoyar la gestión operativa de los incidentes de seguridad que afecten a su ámbito, facilitando la información necesaria y coordinándose con los responsables correspondientes

- Colaborar en la aplicación práctica de los requisitos normativos en materia de Seguridad de la Información y protección de datos personales, prestando apoyo operativo a los Responsables del Tratamiento y a la persona Delegada de Protección de Datos.

- Proponer mejoras operativas en materia de seguridad de la información y protección de datos personales, basadas en el conocimiento del funcionamiento real de los servicios y procesos de su ámbito

- Colaborar en la identificación de tratamientos de datos personales en su ámbito, así como en la gestión de riesgos, incluyendo la realización de análisis de riesgos y evaluaciones de impacto cuando proceda (EIPD)

- Apoyar la detección y gestión de brechas de seguridad de datos personales, facilitando la aplicación de las medidas técnicas y organizativas en materia de protección de datos.

- Actuar como punto de contacto operativo en materia de protección de datos dentro de su ámbito, en coordinación con los responsables correspondientes.

2.4.2. Responsable del Sistema (RSIS)

El Responsable del Sistema (RSIS) es la persona encargada de la operación, administración y mantenimiento de los sistemas de información, de conformidad con las medidas técnicas y organizativas determinadas por el Responsable de Seguridad y las directrices establecidas en el modelo de gobierno de la seguridad.

El Responsable del Sistema ejerce sus funciones durante todo el ciclo de vida del sistema, asegurando su funcionamiento conforme a los requisitos de seguridad, disponibilidad y continuidad definidos por la organización.

2.4.2.1. Funciones Generales del Responsable del Sistema

Las funciones del Responsable de Sistema serán las siguientes:

- Operar y mantener los sistemas de información durante todo su ciclo de vida, aplicando las medidas técnicas y organizativas de seguridad establecidas por los órganos competentes

- Implementar y mantener las salvaguardas de seguridad necesarias para proteger los sistemas frente a amenazas internas y externas, verificando periódicamente su correcto funcionamiento

- Ejecutar las actualizaciones, correcciones y mejoras técnicas necesarias, asegurando la aplicación oportuna de parches de seguridad y la adecuada configuración de los sistemas.

- Aplicar las medidas correctoras derivadas de auditorías de seguridad, informes de evaluación y planes de mejora aprobados.

- Colaborar en la detección, análisis y resolución de incidentes de Seguridad de la Información, aportando soporte técnico para la contención, mitigación y recuperación de los sistemas afectados.

- Ejecutar los procedimientos de continuidad del negocio y recuperación ante desastres (BCP/DRP) que resulten de aplicación a los sistemas bajo su responsabilidad, conforme a los planes aprobados.

- Facilitar información técnica, evidencias y datos relevantes para el seguimiento del estado de seguridad de los sistemas, las auditorías, los análisis de riesgos y la gestión de incidentes.

2.4.3. Responsable de Seguridad Física (RSEF)

El Responsable de Seguridad Física (RSEF) será responsable de definir, implantar y gestionar los requisitos de protección de las instalaciones y de los activos físicos de la DFA dentro de su ámbito de competencia, de acuerdo con las directrices establecidas por el Responsable de Seguridad.

Garantizará que las medidas de seguridad física contribuyan a la protección integral de los sistemas y servicios, apoyando la resiliencia operativa y la continuidad de la actividad

2.4.3.1. Funciones Generales del Responsable de Seguridad Física

Las funciones del Responsable de Seguridad Física (RSEF) serán las siguientes:

- Definir los requisitos de seguridad física aplicables a las instalaciones, dependencias y activos físicos bajo su ámbito de competencia, de conformidad con las directrices y criterios establecidos por el Responsable de Seguridad y la normativa aplicable.

- Colaborar con el Responsable de Seguridad para contribuir a la coherencia e integración entre la seguridad física y las políticas y medidas de seguridad lógica.

- Gestionar y supervisar los sistemas, instalaciones y emplazamientos, en especial las Zonas de Acceso Restringido (ZAR), en lo relativo a las medidas de seguridad física y al control de acceso de personas.

- Mantener y verificar, en coordinación con las áreas competentes, la relación de personas autorizadas a acceder a las distintas áreas y la coherencia con los registros de entradas y salidas.

- Colaborar en los análisis de riesgos, aportando la información de amenazas, vulnerabilidades e impactos asociados a los entornos físicos.

- Supervisar las actuaciones que se realicen sobre el equipamiento de los CPDs (instalación, modificación, retirada), así como el control y registro de entradas y salidas.

- Realizar inspecciones periódicas de seguridad física y colaborar en las auditorías correspondientes, proponiendo mejoras cuando se detecten deficiencias o riesgos.

- Impulsar y gestionar acciones de formación y concienciación del personal y visitantes en materia de seguridad física, incluyendo protocolos de acceso, evacuación y actuación ante incidentes.

- Participar en la gestión y respuesta ante incidentes de seguridad física, colaborando con los órganos responsables para mitigar impactos y facilitar la continuidad operativa.

- Mantener actualizados los procedimientos y protocolos de seguridad física, asegurando su alineación con las normativas internas y externas aplicables.

- Colaborar en la planificación y ejecución de ejercicios de simulación relacionados con la seguridad física.

- Coordinar y supervisar, en su ámbito de competencia, los aspectos de seguridad física asociados a proveedores y servicios externos.

2.4.4. Personas Usuarias (PU)

Serán todas aquellas personas, internas o externas, que dispongan de acceso autorizado a los sistemas de información de la DFA, con independencia del tipo de relación que mantengan con la organización.

Las personas usuarias serán responsables de cumplir las medidas de Seguridad de la Información establecidas en las políticas y normas de la DFA, así como en el resto de legislación y normativa aplicable.

En el desempeño de sus funciones, deberán utilizar los sistemas de información de forma segura y diligente, contribuyendo a la protección de la información gestionada y preservando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

2.4.4.1. Funciones Generales de las Personas Usuarias

Las funciones generales de los usuarios son:

- Conocer y cumplir con los principios de seguridad definidos en la Política Corporativa de Seguridad de la Información, así como las obligaciones establecidas

en la Norma de Uso de los Sistemas de Información y el resto de las políticas, normativas y legislación aplicable.

- Conocer y cumplir los procedimientos que les resulten de aplicación, con el fin de garantizar la protección de la información y de los sistemas que utilicen en el desempeño de sus funciones y obligaciones.

- Participar en las acciones de formación y concienciación en materia de Seguridad de la Información organizadas por la DFA.

- Informar de manera inmediata de cualquier sospecha, mal uso o incidente de seguridad que pueda comprometer la Seguridad de la Información.

- Colaborar con la persona Responsable de Seguridad y las personas Referentes de Seguridad, conforme a los procedimientos establecidos, la implantación y refuerzo de las medidas de protección.

- Mantener la confidencialidad y seguridad de las credenciales de acceso, haciendo un uso diligente de las mismas y utilizando métodos seguros para su gestión.

2.5. Mecanismos de Coordinación y Resolución de Conflictos

En aquellas situaciones en las que surjan discrepancias, solapamientos o controversias relacionadas con el ejercicio de las funciones asignadas a los distintos roles definidos en el presente organigrama —tanto en el ámbito de la seguridad de la información como en el de la protección de datos personales—la responsabilidad de dirimir y resolver dicho conflicto recaerá en el Comité Corporativo de Seguridad y Privacidad (CCSP).

Asimismo, y con el fin de garantizar una adecuada coordinación de las actividades, procesos y medidas de seguridad, se actuará conforme a las directrices y acuerdos adoptados por el Comité Corporativo de Seguridad y Privacidad, que ejercerá funciones de orientación estratégica y alineación global, correspondiendo al Responsable de Seguridad la coordinación operativa y técnica de las actuaciones que resulten necesarias.

Anexo 1: Asignación de roles de Seguridad y Protección de Datos – Nombramientos

La asignación de roles de seguridad se llevará a cabo por los siguientes perfiles:

- Los miembros del **Comité Corporativo de Seguridad y Privacidad** son designados por el **Consejo de Gobierno**.

- **La figura del Responsable de Seguridad (RSEG)** es designado de conformidad con lo establecido en el Decreto de estructura vigente, y será la persona que, dentro de la estructura centralizada de la Diputación Foral de Álava, asuma las funciones, competencias y atribuciones definidas para este rol.

- **La figura del Responsable de Seguridad Física (RSFIS)** es designado a propuesta del Comité Corporativo de Seguridad y Privacidad y será la persona que, dentro de la estructura centralizada de la Diputación Foral de Álava, reúna las funciones, competencias y atribuciones establecidas para este rol.

- **La figura del Responsable de la Información (RINF)** este rol será asumido por las personas titulares de las Direcciones bajo cuya responsabilidad se gestione la información correspondiente.

- **La figura del Responsable de Tratamiento (RTDP)** este rol será asumido por las personas titulares de las Direcciones bajo cuya responsabilidad se lleven a cabo los correspondientes tratamientos, de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y la normativa aplicable.

- **La figura del Responsable del Servicio (RSER)** este rol será asumido por las personas titulares de las Direcciones bajo cuya responsabilidad se gestione la información correspondiente.

- **La figura del Responsable del Sistema** es designado a propuesta del Comité Corporativo de Seguridad y Privacidad y será la persona que, dentro de la estructura centralizada de la Diputación Foral de Álava, reúna las funciones, competencias y atribuciones establecidas para este.

- **La figura del Responsable de Servicios Comunes (RSERC)** es designado a propuesta del Comité Corporativo de Seguridad y Privacidad y será la persona que, dentro de la estructura centralizada de la Diputación Foral de Álava, reúna las funciones, competencias y atribuciones establecidas para este rol.

- **La figura del Referente de Seguridad y Protección de Datos (REFS)** este rol será asumido por las jefaturas de cada servicio y/o por las personas expresamente nombradas al efecto, que, en el ámbito de la jefatura del departamento correspondiente, reúnan las funciones, competencias y atribuciones establecidas para este rol.

- **La figura del Delegado de Protección de Datos (DPD)** será designado por la organización, de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y la normativa aplicable.

Cada miembro del Comité Corporativo de Seguridad y Privacidad contará con un voto para la designación de responsables, independientemente de que la persona ejerza múltiples roles.

La revisión de la designación de roles se realizará cuando haya cambios en la dirección, que puedan impactar en las funciones de los integrantes o cuando el puesto del rol designado quede vacante.

Asimismo, se podrá llevar a cabo la sustitución de los responsables designados en caso de ausencias prolongadas o aquellas de menor duración que puedan generar ineficiencias en el desempeño de sus funciones, afectando al sistema.

Anexo 2: Asignación de roles de Seguridad y Protección de Datos – RACI Figuras

Responsabilidad	RSEG	RSEF	RINF	RTDP	RSER	RSERC	RSIS	REFS	DPD	PU
Organización Corporativa de Seguridad	C	C	I	I	I	I	I	I	I	I
Política Corporativa de Seguridad de la Información	R	I	C	C	C	C	C	I	I	I
Objetivos y planes gestión de seguridad	R	C	C	C	C	C	C	I		I
Niveles de seguridad requeridos por la Información	R		A	A	I	I	C	I		
Niveles de seguridad requeridos por el Servicio	R		I	I	A	A	C	I		
Determinación de la categoría del sistema	A / R		I	I	I	I	I	I		
Análisis de Riesgos	R	C	I	I	I	I	C	C		
Declaración de Aplicabilidad	A / R	I	I	I	I	I	C	I		
Dotación de recursos	C	C	C	C	I	I	I			
Configuración de seguridad	A		I	I	I	I	R	I		
Aceptación del riesgo residual	R	C	C	C	C	C	C	I		
Normativa de seguridad	A / R	C	C	C	C	C	C	I		I
Procedimientos de seguridad	A / R	I	I	I	I	I	A	I		I
Contactos con grupos interés	A / R		I	I	I	I	I			
Implantación de las medidas de seguridad	C	I	I	I	I	I	R	I		I

www.araba.eus
D.L.: VI-1/1958 ISSN: 2254-8432
2026-02300
48/51

Responsabilidad	RSEG	RSEF	RINF	RTDP	RSER	RSERC	RSIS	REFS	DPD	PU
Supervisión de las medidas de seguridad	A / R	C	C	C	C	C	C	I		
Estado de seguridad del sistema	A / R		I	I	I	I	I	I		
Acuerdo nivel servicio seguridad	A	I	C	C	R	R	I	I		
Gestión de RGPD	C		I	R				I	C	I
Planes de mejora de la seguridad	A / R	I	I	I	I	I	C		I	
Planes de concienciación y formación	A / R	I	I	I	I	I	C			I
Gestión de incidentes	A / R		I	I	I	I	C	I	I	I
Gestión brechas de seguridad datos personales	C		I	R				C	C	
Planes de continuidad de negocio	C	I	I	I	A / R	A / R	C	I	C	I
Suspensión cautelar del servicio	A		I	I	C	C	R			I
Seguridad en el ciclo de vida	C		I	I	I	I	A / R			I

R: Responsable / **A**: Aprobador / **C**: Consultado / **I**: Informado

RSEG: Responsable de Seguridad / **RSEF**: Responsable de Seguridad Física / **RINF**: Responsable de la Información / **RTDP**: Responsable del Tratamiento de Datos Personales / **RSER**: Responsable del Servicio / **RSERC:** Responsable de Servicios Comunes / **RSIS**: Responsable del Sistema / **REFS**: Referentes de Seguridad y Protección de Datos / **DPD**: Delegado de Protección de Datos / **PU**: Personas Usuarias

www.araba.eus
D.L.: VI-1/1958 ISSN: 2254-8432
2026-02300
49/51

Anexo 3: Asignación de roles de Seguridad – RACI Comités

Responsabilidad	CCSP	CAS
Organización Corporativa de Seguridad	A / R	I
Política Corporativa de Seguridad de la Información	A	I
Objetivos y planes gestión de seguridad	A	I
Niveles de seguridad requeridos por la Información	I	I
Niveles de seguridad requeridos por el Servicio	I	I
Determinación de la categoría del sistema		
Análisis de Riesgos	A	I
Declaración de Aplicabilidad		I
Dotación de recursos	A / R	I
Configuración de seguridad		
Aceptación del riesgo residual	A	I
Normativa de seguridad	I	I
Procedimientos de seguridad	I	I
Contactos con grupos interés	I	I
Implantación de las medidas de seguridad		I

www.araba.eus
D.L.: VI-1/1958 ISSN: 2254-8432
2026-02300
50/51

Responsabilidad	CCSP	CAS
Supervisión de las medidas de seguridad	I	I
Estado de seguridad del sistema	I	I
Acuerdo nivel servicio seguridad	C	I
Gestión de RGPD	I	I
Planes de mejora de la seguridad	I	I
Planes de concienciación y formación	C	I
Gestión de incidentes	I	I
Planes de continuidad de negocio	C	I
Suspensión cautelar del servicio	I	I
Seguridad en el ciclo de vida		

R: Responsable / **A**: Aprobador / **C**: Consultado / **I**: Informado

CCSP: Comité Corporativo de Seguridad y Privacidad / **CAS**: Comité Asesor Técnico de Seguridad

www.araba.eus
D.L.: VI-1/1958 ISSN: 2254-8432
2026-02300
51/51