I.Disposiciones Generales

CONSEJERÍA DE DESARROLLO AUTONÓMICO

Decreto 4/2023, de 15 de febrero, por el que se aprueba la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de La Rioja

202302160097290 I.14

Uno de los objetivos del Gobierno de La Rioja es la consecución de una administración innovadora y abierta que ofrezca a la sociedad servicios de calidad, eficientes, eficaces y seguros. Para ello, debe colaborar con su entorno, impulsar o activar a los ciudadanos para que actúen en el ámbito público, contando con las personas como protagonistas del cambio y todo ello basado en los nuevos valores de gobernanza: apertura, orientación a resultados, transparencia e innovación.

En el ejercicio de sus responsabilidades, la relación de la administración con los ciudadanos u otros entes, se produce mediante diversos medios electrónicos y sistemas tecnológicos con los que la Administración del Gobierno de La Rioja obtiene, trata, transfiere o intercambia información, al mismo tiempo que la almacena.

El Gobierno de La Rioja depende de los sistemas TIC (Tecnologías de Información y Comunicación) para alcanzar sus objetivos. Estos sistemas deben ser administrados con meticulosidad, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, autenticidad, trazabilidad y confidencialidad de la información tratada o los servicios prestados.

La necesidad de proteger esa información adquiere aún más fuerza en el momento actual, cuando el uso de las tecnologías de la información y de la comunicación es intensa por parte de las administraciones públicas, que además impulsan su uso a través de las normas que regulan el funcionamiento de su actividad, y cuando los riesgos y las amenazas son grandes.

Así, La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas consolida, en su artículo 14, el derecho de los ciudadanos a relacionarse, preferentemente por medios electrónicos, con las administraciones públicas, siendo, en algunos casos, obligatoria la utilización de medios electrónicos para trámites administrativos a determinados colectivos (personas jurídicas, entidades sin personalidad jurídica, profesionales colegiados, etc.), según las normas de desarrollo.

El Esquema Nacional de Seguridad (ENS) actualizado y aprobado por Real Decreto 311/2022, de 3 de mayo, obliga a los órganos superiores de las administraciones públicas a dotarse formalmente de una política de seguridad, que deberá atenerse a los principios básicos y requisitos mínimos que se relacionan en los capítulos II y III de ese Real Decreto.

Además, la Política de Seguridad de la Información obedece también a la exigencia del cumplimiento de diferentes normas legales y reglamentarias en materia de Seguridad de la Información, como el 13.h) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público o por el Real Decreto-ley 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información y el Real Decreto 43/2021, de 26 de enero, que lo desarrolla. El objeto de este conjunto normativo, junto con el mencionado ENS, es el establecimiento de los principios básicos y requisitos mínimos de una política de seguridad en la utilización de medios electrónicos, que permita una adecuada protección de la información y la creación de las condiciones necesarias de confianza en el uso de los servicios electrónicos que prestan las administraciones.

Así mismo, 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 datos, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establecen una serie de garantías, en defensa del derecho fundamental a la protección de los datos de carácter personal.

Esta norma, que ahora se aprueba, viene a sustituir a la anterior aprobada por Decreto 96/2020, de 4 de noviembre, por el que se aprueba la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de La Rioja y a adaptarla a los cambios normativos ocurridos tras su aprobación.

El artículo 8.uno.1 y 2 de la Ley Orgánica 3/1982, de 9 de junio, del Estatuto de Autonomía de La Rioja establece que corresponde a la Comunidad Autónoma de La Rioja la competencia exclusiva en las materias de organización, estructura, régimen y funcionamiento de sus instituciones de autogobierno, y en el procedimiento administrativo derivado de las

especialidades de la organización propia de La Rioja. Por ello, en ejercicio de la potestad reglamentaria atribuida al Gobierno en el artículo 24 del citado Estatuto de Autonomía, resulta procedente la elaboración del reglamento propuesto, que dispone de la suficiente cobertura legal, y entra dentro del ámbito competencial de la Comunidad Autónoma de La Rioja.

En su virtud, el Consejo de Gobierno, a propuesta del Consejero de Desarrollo Autonómico, y previa deliberación de sus miembros, en su reunión del día 15 de febrero de 2023, acuerda aprobar el siguiente,

DECRETO

Artículo único. *Aprobación Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de La Rioja.*

Se aprueba la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de La Rioja en los términos recogidos en el Anexo.

Disposición adicional primera. *Deber de colaboración.*

Todos los órganos y unidades administrativas de la Administración de la Comunidad Autónoma de La Rioja deberán colaborar en las acciones de implementación de esta política de seguridad.

Disposición adicional segunda. *Relación con terceros.*

Cuando por razón de su contenido resulte aplicable, los contratos o convenios que se suscriban a partir de la entrada en vigor de este Decreto deberán contener una cláusula en la que se establezca la obligación de cumplir esta política y el sistema de verificación de su cumplimiento e incluir un acuerdo de confidencialidad.

Disposición derogatoria única. *Derogación normativa.*

Queda derogado el Decreto 96/2020, de 4 de noviembre, por el que se aprueba la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de La Rioja.

Disposición final primera. *Facultad de desarrollo.*

Se faculta al titular de la Consejería con competencias en materia de tecnologías de la información para dictar cuantas disposiciones exija la aplicación y ejecución de este Decreto.

Disposición final segunda. *Vigencia.*

El presente Decreto entrará en vigor el día siguiente al de su publicación en el Boletín Oficial de La Rioja.

Logroño a 15 de febrero de 2023.- La Presidenta, Concepción Andreu Rodríguez.- El Consejero de Desarrollo Autonómico, José Ángel Lacalzada Esquivel.

ANEXO

Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de La Rioja

Introducción.

La información constituye un activo de primer orden para el Gobierno de La Rioja, ya que resulta imprescindible para la prestación de los servicios públicos. Por su parte, las tecnologías de la información y las comunicaciones se han hecho imprescindibles para las administraciones públicas ya que contribuyen a la obtención, intercambio, tratamiento y almacenamiento de esa información.

Sin embargo, las mejoras que aportan las TIC al tratamiento de la información, vienen acompañadas de nuevos riesgos. Por esa razón es necesario introducir medidas específicas para proteger tanto la información, como los servicios que dependen de ella.

La seguridad de la información, tiene como objetivo proteger la información y los servicios, reduciendo los riesgos a los que están sometidos hasta un nivel que resulte aceptable. El presente documento establece la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de La Rioja que constituye el marco de referencia orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad establecidos en el Esquema Nacional de Seguridad.

Con ello se pretende lograr el alineamiento estratégico de la gestión de la seguridad de la información con las normas internacionales y las regulaciones legislativas existentes en la materia.

1. *Misión y objetivos de la Política de Seguridad de la Información.*

Uno de los objetivos fundamentales, de la implantación de esta Política de Seguridad, es establecer las bases sobre las que, tanto empleados públicos como ciudadanos, puedan acceder a los servicios públicos en un entorno seguro y de confianza.

La Política de Seguridad de la Información define el marco global para la gestión de la seguridad de la información, protegiendo todos los activos de información y garantizando la continuidad en el funcionamiento de los sistemas. Se pretende, de esta forma, minimizar los riesgos derivados de una posible falla en la seguridad y asegurar el cumplimiento de los objetivos del Gobierno de La Rioja ante un hipotético incidente de seguridad de la información.

Para ello, se establecen los siguientes objetivos generales en materia de seguridad de la información:

1) Contribuir desde la gestión de la seguridad al cumplimiento de la misión y objetivos establecidos por el Gobierno de La Rioja.

2) Disponer de las medidas de control necesarias para garantizar el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos o telemáticos.

3) Asegurar la accesibilidad, confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

4) Asegurar la prestación continuada de los servicios, tanto de forma preventiva como de forma reactiva ante los incidentes de seguridad.

5) Proteger los activos de información de la Administración de la Comunidad Autónoma de La Rioja y la tecnología que los soporta frente a cualquier amenaza, intencionada o accidental, interna o externa, con el fin de asegurar la confidencialidad, integridad y disponibilidad de los mismos.

Esta Política de Seguridad asegura un compromiso continuo y manifiesto del Gobierno de La Rioja y todas sus instituciones, para la difusión y consolidación de la cultura de la seguridad.

El Gobierno de La Rioja debe estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo 8 del ENS.

1.1 Prevención.

El Gobierno de La Rioja debe evitar o al menos prevenir, en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y

riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, la organización a través de los responsables designados debe:

- Autorizar los sistemas antes de entrar en operación.

- Evaluar regularmente la seguridad, incluyendo los cambios de configuración realizados de forma rutinaria.

- Solicitar la revisión o auditoría periódica por parte de terceros con el fin de obtener una evaluación independiente.

1.2 Detección.

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el artículo 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 9 del ENS. Se deben establecer mecanismos de detección, análisis y reporte que lleguen a las o los responsables regularmente y en el momento en que se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

1.3 Respuesta.

En el caso de que se materializara un incidente de seguridad, el Gobierno de La Rioja debe:

- Establecer mecanismos para responder eficazmente a ese incidente de seguridad.

- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros organismos relacionados con el Gobierno de La Rioja.

- Establecer protocolos para el intercambio de información relacionada con el incidente entre el Gobierno de La Rioja y los órganos de control y supervisión nacionales y con cualquier otra institución u organismo que pueda colaborar en la respuesta a los incidentes. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT) nacionales.

1.4 Recuperación.

Para garantizar la disponibilidad de los servicios esenciales, el Gobierno de La Rioja debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

2. *Alcance.*

Esta Política de seguridad se aplicará al Sector Público de la Comunidad Autónoma de La Rioja.

A estos efectos se entiende por Administración de la Comunidad Autónoma de La Rioja:

a) La Administración General de La Rioja.

b) Los Organismos Públicos vinculados o dependientes de la Administración General.

c) Otros entes del sector público de La Rioja que usen recursos o sistemas de información del Gobierno de La Rioja: fundaciones, consorcios y sociedades públicas.

Los entes integrantes del sector público de la Comunidad Autónoma de La Rioja que no utilicen los recursos ni los sistemas de información del Gobierno de La Rioja podrán aplicar esta política de seguridad cuando así lo acuerden o lo establezcan sus normas internas de funcionamiento.

Esta política afectará a la información y datos tratados por medios electrónicos y en soporte papel que gestiona la Administración de la Comunidad Autónoma de La Rioja en el ejercicio de sus competencias.

3. *Marco normativo.*

Sin carácter exhaustivo, la legislación en materia de seguridad de la información que debe servir de referencia es la siguiente:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE.

- Ley Orgánica 3/1982, de 9 de junio, de Estatuto de Autonomía de La Rioja.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Personales y Garantía de los Derechos Digitales.

- Ley 39/2105, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

- Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

- Decreto 46/2020, de 3 de septiembre, por el que se establece la estructura orgánica de la Consejería de Desarrollo Autonómico y sus funciones en desarrollo de la Ley 3/2003, de 3 de marzo, de Organización del Sector Público de la Comunidad Autónoma de La Rioja.

4. *Revisión de la política.*

La revisión de la Política de Seguridad de la Información deberá garantizar que ésta se encuentra alineada con la estrategia, la misión y visión del Gobierno de La Rioja en materia de seguridad de la información y que asegura el cumplimiento de los objetivos de control establecidos.

En relación a las revisiones que puedan realizarse sobre la redacción del texto que constituye la política de seguridad de la información, se distinguirán tres tipos de actividades:

- Revisiones periódicas, que se realizarán, al menos, con una periodicidad anual.

- Revisiones sistemáticas: Deberán realizarse cuando se detecten incidencias o cambios en el marco legal que puedan cuestionar la validez de dicha Política.

- Revisiones no planificadas: Estas revisiones deberán realizarse en respuesta a cualquier evento o incidente de seguridad que pudiera suponer un incremento significativo del nivel de riesgo actual o que haya causado un impacto en la seguridad de la información del Gobierno de La Rioja.

5. *Organización interna de la seguridad.*

La estructura organizativa para la gestión de la seguridad de la información está integrada de la forma que se detalla a continuación:

- Comité de Seguridad de la Información.

- Responsable de la Información.

- Responsable del Servicio.

- Responsable de Seguridad.

- Responsable del Sistema.

5.1. Comité de Seguridad de la Información.

5.1.1. El Comité de Seguridad de la Información del Gobierno de La Rioja, en adelante CSI-CAR, se compone de los siguientes miembros:

a) Presidente: El titular de la Dirección General competente en materia de tecnologías de la información y las comunicaciones. En caso de vacante, ausencia o enfermedad será sustituido por el miembro del Comité de mayor jerarquía, antigüedad y edad, por ese orden.

b) Vocales: Los titulares de cada una de las Secretarías Generales Técnicas, el Delegado de Protección de Datos de la Administración General y Organismos Públicos de la Comunidad Autónoma de La Rioja y el responsable de seguridad de la Dirección General competente en materia de tecnologías de la información y las comunicaciones.

c) El Secretario será nombrado por el titular de la Dirección General competente en materia de tecnologías de la información y la comunicación, entre personal de la misma Dirección General. En caso de vacante, ausencia o enfermedad, su suplente será designado de igual modo por el mismo órgano.

5.1.2. Tanto los titulares de cada una de las Secretarías Generales Técnicas, como las personas que ocupen los puestos de Delegados de Protección de Datos, podrán designar los correspondientes asesores que acudirán a las reuniones con voz, pero sin voto. El Presidente del Comité podrá proponer otras personas que podrán asistir a las reuniones en calidad de asesores con voz, pero sin voto.

5.1.3. Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, podrán crearse «Comités de Seguridad delegados», dependientes funcionalmente del CSI-CAR que serán responsables en su ámbito de las actuaciones que se les deleguen.

5.1.4. Al Comité de Seguridad de la Información del Gobierno de La Rioja le corresponden funciones de asesoramiento, consultoría y propuesta en materia de seguridad de la información.

En particular le corresponde:

a) Informar regularmente del estado de la seguridad de la información al Gobierno de La Rioja.

b) Promover la mejora continua del sistema de gestión de la seguridad de la información.

c) Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, evitando duplicidades.

d) Elaborar y revisar regularmente la Política y Organización de la Seguridad de la Información, para que sea aprobada por el Gobierno de La Rioja.

e) Proponer la aprobación de la normativa de seguridad de la información.

f) Promover la realización de las auditorías periódicas, que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

g) Proponer planes de mejora de la seguridad de la información de la organización.

h) Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos de tecnologías de la información, desde su especificación inicial hasta su puesta en operación y posterior mantenimiento, así como en la preservación de la información, que sea requerida tras el cese en la utilización del mismo.

i) Divulgar la Política de Seguridad de la Información y normativas e instrucciones de seguridad de la información aprobadas.

5.1.5. El Comité de Seguridad de la Información del Gobierno de La Rioja se reunirá, con carácter ordinario, una vez al semestre y podrá reunirse con carácter extraordinario en alguno de los siguientes supuestos:

a) A instancia del Presidente.

b) Cuando aparezcan incidencias de seguridad graves o surjan nuevas necesidades de seguridad, que requieran la participación de los componentes del Comité.

5.1.6. El Comité de Seguridad de la Información, ajustará su funcionamiento a las previsiones relativas a los órganos colegiados contenidas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

5.2. Responsable de la información.

El Responsable de la Información, será el titular del órgano administrativo con competencia suficiente para decidir sobre el uso que se haga de una cierta información y, por tanto, de su protección, y determinará dentro del marco establecido en el Anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, los requisitos de seguridad de la información tratada. A tal efecto:

a) Determinará los requisitos de seguridad que deban ser garantizados en el tratamiento de la información de la que él es responsable.

b) Valorará, para cada información contemplada en el análisis de riesgos, las diferentes dimensiones de la seguridad.

c) Aceptará los riesgos residuales, calculados en el análisis de riesgos respecto de la información.

d) Realizará el seguimiento y control de los riesgos con la ayuda del Responsable de Seguridad.

5.3. Responsable del servicio.

El Responsable del Servicio, será el titular del órgano administrativo con competencia suficiente para decidir sobre la finalidad y prestación del servicio, y determinará, dentro del marco establecido en el Anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, los requisitos de seguridad de los servicios prestados. A tal efecto:

a) Realizará, junto a los Responsables de la Información y el Responsable de Seguridad, los preceptivos análisis de riesgos y seleccionarán las salvaguardas que se han de implantar.

b) Aceptará los riesgos residuales, respecto de la información, calculados en el análisis de riesgos.

c) Realizará el seguimiento y control de los riesgos, con la participación del Responsable de Seguridad.

d) Suspenderá, de acuerdo con el Responsable de la Información y el Responsable de Seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

5.4. Responsable de seguridad.

El Responsable de Seguridad será designado por el titular del órgano con competencias en materia de tecnologías de la información entre personal adscrito a dicho órgano.

Tendrá las siguientes funciones:

a) Mantener la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

b) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.

c) Impulsar el cumplimiento del cuerpo normativo definido en el apartado 3, así como velar por el mantenimiento de la documentación de seguridad y la gestión de mecanismos de acceso a la misma.

d) Mantener un inventario actualizado de las normas de primer y segundo nivel detalladas en el apartado 8, de los nombramientos derivados de la presente orden, así como de los informes de auditorías, autoevaluaciones y análisis de riesgos realizados y de las declaraciones y certificaciones de seguridad.

e) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.

f) Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes de cada período.

g) Promover la mejora continua en la gestión de la seguridad de la información.

h) Impulsar la formación y concienciación en materia de seguridad de la información.

i) Aprobar la declaración de aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.

j) Realizar los preceptivos análisis de riesgos y mantenerlos actualizados según la legislación vigente.

k) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes de auditoría, elaborando las conclusiones a presentar a los Responsables del Servicio y los Responsables de la Información para que adopten las medidas correctoras adecuadas bajo su responsabilidad.

l) Cualesquiera otras funciones que el Real Decreto 311/2022, de 3 de mayo, asigne a los responsables de seguridad.

Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, podrán designarse «responsables de seguridad delegados», dependientes funcionalmente del responsable principal, que serán responsables de las actuaciones que se les deleguen.

5.5. Responsable del sistema.

El Responsable del Sistema, será el titular del órgano con competencias en materia de sistemas y tecnologías de la información, y tiene las siguientes funciones:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.

b) Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.

c) Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

d) Colaborar en la investigación y resolución de incidentes de seguridad.

e) Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el responsable de dicha información o servicio, según proceda, y con el responsable de seguridad.

Cuando lo justifique la complejidad, la separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, el responsable del Sistema podrá designar «responsables de sistema delegados», dependientes funcionalmente del responsable principal, que se harán cargo, en su ámbito competencial, de todas aquellas acciones delegadas por el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información. El responsable principal seguirá siendo el responsable final.

6. *Datos de carácter personal.*

Cuando un sistema al que afecte el Esquema Nacional de Seguridad maneje datos de carácter personal le será de aplicación lo dispuesto en 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 datos, así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en lo que le afecte.

7. *Gestión de riesgos.*

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- Al menos una vez al año (mediante revisión y aprobación formal).

- Cuando cambie la información manejada.

- Cuando cambien los servicios prestados.

- Cuando ocurra un incidente grave de seguridad.

- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, se establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

8. *Instrumentos de desarrollo.*

Se establece un marco normativo en materia de seguridad de la información, estructurado por diferentes niveles, de forma que los objetivos marcados por el presente documento tengan un desarrollo específico.

La política de seguridad estructurará su marco normativo, en los siguientes niveles:

- Primer nivel: Está constituido por la presente Política de Seguridad de la Información que establece los requisitos y criterios de protección de carácter global.

- Segundo nivel: Las normas de seguridad que definen qué hay que proteger y los requisitos de seguridad deseados. El conjunto de todas las normas de seguridad, debe cubrir la protección de todos los entornos de los sistemas de información de la organización. Establecen un conjunto de expectativas y requisitos que deben ser alcanzados para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la política.

- Tercer nivel: Está constituido por procedimientos, guías e instrucciones técnicas en los que se describirá, de forma concreta, cómo proteger lo definido en las normas y las personas o grupos responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento. Son documentos que especifican, cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.

9. *Obligaciones del personal.*

Todo el personal con responsabilidad en el uso, operación o administración de sistemas de tecnologías de la información y las comunicaciones tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad derivada, independientemente del tipo de relación jurídica que les vincule con la Administración General y con sus organismos Públicos.

Todas las personas recibirán formación para el manejo seguro de los sistemas, en la medida en que la necesiten para realizar su trabajo.

La Política de Seguridad estará accesible para todo el personal que preste sus servicios en los órganos y entidades a que se refiere el punto relativo al 'Alcance'.

Con el objetivo de fomentar la 'Cultura de la seguridad', el Comité de Seguridad de la Información promoverá un programa de concienciación continua para formar a todo el personal.

El incumplimiento de la Política de Seguridad y su normativa de desarrollo, dará lugar al establecimiento de medidas preventivas y correctivas encaminadas a salvaguardar y proteger las redes y sistemas de información, sin perjuicio de la correspondiente exigencia de responsabilidad disciplinaria o penal, en su caso.