Agència Tributària Valenciana

Política de Seguridad de la Información

Agència Tributària Valenciana

27 de enero de 2023

Índice

1. Introducción

La Agencia Tributaria Valenciana (en adelante, la Agencia o “ATV”), depende de los sistemas TIC (Tecnologías de la Información y las Telecomunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad de la información tratada o los servicios prestados y estando siempre protegidos contra las amenazas o los incidentes con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información tratada y los servicios prestados.

Para hacer frente a estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), así como realizar un seguimiento continuo de los niveles de prestación de los servicios, monitorizar y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los ciberincidentes para garantizar la continuidad de los servicios prestados.

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

Por tanto, para la Agencia Tributaria Valenciana, el objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible, con la aplicación de las medidas.

2. Misión y servicios prestados

La misión de la Agencia Tributaria Valenciana consiste en coadyuvar al logro de un grado satisfactorio de suficiencia financiera, en aplicación de lo dispuesto en el artículo 67 del Estatut d'Autonomía de la Comunitat Valenciana y en los artículos 1 y 2 de la Ley Orgánica 8/1980, de 22 de septiembre, de Financiación de las Comunidades Autónomas, incrementar la eficacia para allegar los recursos necesarios para el sostenimiento de los gastos públicos, mejorar la prestación del servicio y la calidad en la atención y asistencia al contribuyente, potenciar la colaboración y cooperación interadministrativas y afrontar adecuadamente la labor de control y lucha contra la defraudación fiscal en el ámbito de los tributos gestionados por la Generalitat.

Desde su creación, la ATV queda configurada como un organismo autónomo adscrito a la Conselleria competente en materia de hacienda, con personalidad jurídica propia, autonomía funcional y de gestión, y plena capacidad de actuación en el desarrollo de las funciones asumidas. Le corresponde la aplicación de los tributos y el ejercicio de la potestad sancionadora tanto sobre los tributos propios de la Generalitat como sobre los tributos cedidos por el Estado, en el marco de la vigente Ley Orgánica de financiación autonómica.

La ATV presta los siguientes servicios:

- Facilita información, asistencia y orientación general, sobre sus servicios, oficinas, y organización, en todos sus centros gestores, en horario de atención al público, en el servicio telefónico de información tributaria y en Internet.

- Facilita información tributaria, como pueda ser:

  a) Información y asistencia sobre el cumplimiento de las obligaciones tributarias derivadas de los tributos cuya gestión se le encomienda, previa cita, obtenida por Internet

  b) Información genérica sobre los tributos que gestiona la ATV, y sobre las tasas y otros ingresos de derecho público.

  c) Información sobre el estado de tramitación de los expedientes, previa cita, obtenida por Internet.

  d) Información sobre normativa y doctrina tributaria, novedades fiscales, convenios en vigor, estadísticas tributarias, informes del Ministerio, y beneficios fiscales aplicables.

- Pone a disposición de los ciudadanos diferentes programas informáticos de ayuda para la confección y presentación telemática de declaraciones tributarias, así como ayuda en internet para el cálculo del valor real de bienes inmuebles

urbanos y rústicos, y del valor fiscal de vehículos.

- Asiste e informa en la Campaña del IRPF.
- Facilita a los ciudadanos el pago de deudas mediante i) la habilitación de diferentes medios de pago, ii) la concesión de aplazamientos y fraccionamientos, y, iii) el acuerdo de compensaciones de deudas y pago en especie
- Emite a petición de los interesados diferentes documentos, entre otros:

  a) Certificado de estar al corriente de las deudas tributarias con la Generalitat.

  b) Informe, cuando las leyes o los reglamentos propios de cada tributo así lo prevean, sobre la valoración a efectos fiscales de rentas, productos, bienes, gastos y demás elementos determinantes de la deuda tributaria.

  c) Certificados de los pagos realizados.

- Presta el servicio de registro general.

3. Principios básicos

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

- Seguridad como proceso integral.
- Gestión de la seguridad basada en los riesgos.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua.
- Reevaluación periódica.
- Diferenciación de responsabilidades.

Y por ello, y se desarrollará aplicando los siguientes requisitos mínimos:

- Organización e implantación del proceso de seguridad
- Análisis y gestión de los riesgos
- Gestión de personal
- Profesionalidad

- Autorización y control de los accesos
- Protección de las instalaciones
- Adquisición de productos de seguridad y contratación de servicios seguridad
- Mínimo privilegio
- Integridad y actualización del sistema
- de la información almacenada y en tránsito
- Prevención ante otros sistemas de información interconectados
- Registros de la actividad y detección de código dañino
- Incidentes de seguridad
- Continuidad de la actividad
- Mejora continua del proceso de seguridad

4. Objetivos de la Seguridad de la información

La ATV, establece como objetivos de la seguridad de la información los siguientes:

- Garantizar la calidad y protección de la información.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
- Gestión de activos de información: Los activos de información de la ATV se encontrarán inventariados y categorizados y estarán asociados a un responsable.
- Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un su uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
- 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.
- Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. 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.
- Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, 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.

- 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.
- Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- Garantizar la prestación continuada de los servicios: 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 sus usuarios.
- Protección de datos: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad.
- 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.

5. Alcance

Esta Política se aplicará a los sistemas de información de la ATV, relacionados con el ejercicio de sus competencias y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la ATV. Todos ellos tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y su Normativa de Seguridad derivada, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue al personal afectado.

6. Marco normativo

El marco normativo que aplica a la ATV es aquel que está regido a través de todas aquellas normas que integren la seguridad de la información en el ámbito del servicio que presta la organización, en especial el Esquema Nacional de Seguridad (ENS) y cualquier norma que derive o esté tratada en este.

Se mantendrá un Anexo con la identificación de la normativa aplicable.

7. Organización de la Seguridad de la Información

7.1. Criterios de la Seguridad de la Información

La ATV teniendo en cuenta los artículos 11,12 y 13 del ENS (Real Decreto 311/2022), establece las siguientes acciones para organizar la Seguridad de la Información:

i. Designará roles de seguridad: Responsables unificados de Servicios y de la Información, Responsable de la Seguridad, Responsable del Sistema y Delegado de Protección de Datos.

ii. Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información. Este órgano se denominará Comité de Seguridad de la Información.

7.2. Definición de Roles y Responsabilidades asociados al Esquema nacional de Seguridad

7.2.1. Responsable de la Información y de los Servicios

Serán funciones de los Responsables de la Información y de los Servicios:

- Establecer los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información) y a los Servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del RD ENS, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
- Dictaminar respecto a los derechos de acceso a la información y los servicios.
- Aceptar los niveles de riesgo residual que afectan a la información y los servicios.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo. El cual dará traslado de dichos cambios, al Comité de Seguridad de la Información, en su próxima reunión.
- Tiene la responsabilidad última del uso que se haga de determinados servicios e información y, por tanto, de su protección.

7.2.2. Responsable de la Seguridad de la Información

Serán funciones del Seguridad de la Información (en adelante, Responsable de Seguridad):

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.

- Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias y elaborar documentación del sistema.
- Aprobar la Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad TIC.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.
- Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, la Política de Seguridad de la Información, para su aprobación por Dirección.
- Actuará como Secretario del Comité de Seguridad de la Información, realizando las siguientes funciones:
    - Convocar las reuniones del Comité de Seguridad de la Información.
    - Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
    - Elaborar el acta de las reuniones.
    - Es responsable de la ejecución directa o delegada de las decisiones del Comité.

7.2.3. Responsable del Sistema

Serán funciones del Responsable del Sistema:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad de la Información de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Coordinar las funciones del administrador de la seguridad del sistema:

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
- Informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

7.3. Designación de Roles y Responsabilidades asociados al Esquema nacional de Seguridad

- Responsable de Sistema: Jefatura de Servicio de Teleadministración.
- Responsable de Seguridad de la Información: Jefatura de Departamento de Informática.
- Responsables del Servicio y de la Información: Jefaturas de área de la ATV y Delegado/a de Alicante y Castellón.

7.4. Comité de Seguridad de la Información

En la ATV, se ha creado el Comité de Seguridad de la Información que estará compuesto por los siguientes miembros:

- Presidencia: Subdirección general
- Secretario: Responsable de Seguridad
- Vocales: Responsables del Servicio e Información.

Estos miembros se clasificarán en permanentes o no permanentes atiendo a la obligatoriedad de la participación del Comité de Seguridad de la Información:

- Miembros permanentes:
  - Presidencia
  - Responsable de Sistema
  - Responsable de Seguridad de la Información

    - Asesores que se consideren oportunos para los temas en cuestión con voz, pero sin voto.

- Miembros no permanentes:
    - Responsables del Servicio y de la Información.
    - El Delegado de Protección de datos.
    - Representantes de la ATV, especialistas externos de los sectores público, privado, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

Los Responsables de la Información y los Servicios serán convocados por la presidencia en función de los asuntos a tratar, en representación de los distintos ámbitos o áreas de seguridad TIC de la ATV. Cada área estará representada por un vocal con voto, sin perjuicio de que acudan varios representantes de la misma.

El Delegado de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

El Secretario/a del Comité realizará las convocatorias y levantará actas de las reuniones del Comité de Seguridad. A las sesiones del Comité de Seguridad podrán asistir en calidad de asesores las personas que en cada caso estime pertinentes su Presidente.

7.4.1. Atribuciones del Comité de Seguridad de la Información

Serán funciones del Comité de Seguridad:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución en lo que respecta a la seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar documentación de seguridad de la información.
- Estar permanentemente informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.
- Estar permanentemente informado de la relación de Entidades de Certificación acreditadas y organizaciones, públicas y privadas, certificadas.
- Estar permanentemente informado de la relación de esquemas de certificación de la seguridad con los que la Administración Pública tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.

- Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, a las que su presidente, deberá dar cumplida respuesta.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Atender las inquietudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas, informando regularmente del estado de la seguridad de la información a la Dirección.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Departamentos, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.
- Revisar la Política de Seguridad de la Información previa aprobación por el Órgano Superior.
- Aprobar el Plan de Adecuación para la implantación del ENS.

7.4.2. Periodicidad de las reuniones y adopción de acuerdos

- El Comité de Seguridad de la Información se reunirá, al menos, una vez al año, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.
- En cualquier caso, las reuniones se convocarán por su Presidencia, a través del Secretario, a su iniciativa o por mayoría de sus miembros permanentes.
- Las decisiones se adoptarán por consenso de los miembros permanentes.

7.5. Grupo de Trabajo TIC

Dentro de la estructura de gobernanza de la ciberseguridad se constituye la **Oficina de Seguridad TIC**, cuyas competencias estarán relacionadas con las siguientes áreas de trabajo: adecuación al ENS, normativa y gestión de riesgos, análisis y mejora continua, seguridad en las interconexiones y conectividad y otras funciones conexas o concordantes. Para su **composición** se propone:

- Responsable de Seguridad
- Responsable del Sistema
- Delegado /a de la Secretaría General
- Consultor/a externo experto en ENS como miembro no permanente
- Todos aquellos administradores especialistas de seguridad (interno o externos a la ATV) que el Responsable de Seguridad determine que sean necesarios como miembro no permanentes.

7.5.1. Atribuciones del Grupo de Trabajo TIC

Las **funciones del Grupo de Trabajo TIC** serán, entre otras que les puedan ser encomendadas por el Comité de Seguridad:

- Gestión y operativa de la seguridad del Proyecto de Adecuación, Implantación y gestión de la Conformidad en el ENS, análisis y gestión de riesgos, explotación, normativa y mantenimiento.
- Redacción y presentación de propuestas al Comité de Seguridad TIC. Elaborará los aspectos relacionados con la ciberseguridad y los debatirá en primera instancia, para ser trasladados al Comité.
- Promover de la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su traslado al Comité de Seguridad TIC para su revisión y posterior aprobación del órgano superior.
    - Elaborar la normativa de Seguridad de la Información para su aprobación por el Responsable de Seguridad, con conocimiento del Comité
    - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
    - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información y protección de datos.
    - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
    - Proponer planes de mejora de la seguridad de la información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
    - Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.
    - Promover la realización de las auditorías periódicas ENS que permitan verificar el cumplimiento de las obligaciones de la ATV en materia de seguridad de la Información y protección de datos.

7.5.2. Periodicidad de las reuniones y adopción de acuerdos

- Se reunirá, al menos, una vez al trimestre y siempre antes de las celebraciones del Comité de Seguridad TIC.
- Se recabará los acuerdos alcanzados, de los que dará cuenta al Comité de Seguridad TIC, para su aprobación, en su caso.
- La Oficina podrá desarrollar sus funciones en pleno o en Grupos de Trabajo para el análisis y realización de propuestas específicas. Las propuestas planteadas en la Oficina de Seguridad TIC serán sometidas a análisis, debate y aprobación, si procede, por parte del Comité de Seguridad TIC.

7.6. Procedimiento de designación

7.6.1. Procedimiento de designación Comité de Seguridad de la Información

- La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política, se realizará por la Dirección General de la ATV, mediante la correspondiente Instrucción.
- Los roles nombrados se renovarán anualmente de forma automática. Las bajas o modificaciones en los roles designados, se comunicarán al Comité y se seguirán los cauces establecidos para la designación del nuevo responsable.

7.6.2. Procedimiento de designación Grupo de Trabajo TIC

- El nombramiento formal del Grupo de Trabajo TIC y de sus integrantes se formalizará a través de un acta del Comité de Seguridad de la Información.

8. Datos personales

La ATV, solo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de las normativas de Protección de Datos.

La ATV, publicará su Registro de Actividades de Tratamiento y realizará la gestión de riesgos a través de Análisis de Riesgos y EPID, en el caso que fuese necesario en la organización.

9. Obligaciones del personal

Todo el personal de la ATV, tanto externo como interno, que interactúe con el sistema de información deberá de cumplir con la presente política de seguridad de la información.

10. Gestión de riesgos

Todos los sistemas afectados por la presente Política de Seguridad de la Información están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de la Seguridad será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.
- El Comité de Seguridad de la Información procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los Anexos I y II del Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, Guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

En particular, para realizar el análisis de riesgos, como norma general se utilizará una metodología reconocida de análisis y gestión de riesgos.

7.1. Riesgos que se derivan del tratamiento de datos personales

Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

11. Documentación Complementaria

La presente Política de Seguridad de la Información será complementada con documentos más precisos (normas, guías y procedimientos de seguridad) que ayudan a llevar a cabo lo propuesto.

El cuerpo normativo se desarrollará en tres niveles:

a) Primer nivel normativo: constituido por la presente Política de Seguridad de la Información.

b) Segundo nivel normativo: constituido por las normas de seguridad derivadas de las anteriores con el objetivo de indicar el uso correcto de aspectos concretos del sistema de gestión de seguridad de la información.

c) Tercer nivel normativo: constituido por procedimientos de seguridad, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde a la Dirección General de la ATV, la aprobación de la Política de Seguridad de la Información y siendo el Comité de Seguridad de la Información el órgano responsable de la aprobación y difusión de los restantes documentos propios de la ATV. La ATV complementará su cuerpo normativo con documentos propios de la Dirección General de Tecnologías de la Información y las Comunicaciones (en adelante DGTIC), debido a las competencias horizontales que ostenta en Tecnologías de la Información y la Comunicación (TIC) de la Generalitat.

12. Terceras partes

Cuando la ATV, preste servicios a otros organismos o maneje información de otros organismos, se les hará participe de esta Política de Seguridad de la Información. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la ATV, utilice servicios de terceros o ceda información a terceros, se les hará participe de esta Política de Seguridad y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de esta Política de Seguridad de la Información no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

13. Mejora continua

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas.

Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

a) Revisión de la Política de Seguridad de la Información.
b) Revisión de los servicios e información y su categorización.
c) Ejecución con periodicidad anual del análisis de riesgos.
d) Realización de auditorías internas o, cuando procedan, externas.
e) Revisión de las medidas de seguridad.
f) Revisión y actualización de las normas y procedimientos.

14. Aprobación y entrada en vigor

Esta Política de Seguridad de la Información, será efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por el Consejo Rector de la Agencia Tributaria Valenciana, de acuerdo con lo establecido en el artículo 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

El texto ha sido aprobado en el Consejo Rector de la Agencia Tributaria Valenciana el 31 de enero de 2023.