POL – 0001

Política de Seguridad de la Información de la DGT

Ámbito

Dirección General de Tráfico

Autor:

GI DGT Área de Seguridad TIC

Gerencia de Informática

Dirección General de Tráfico

JOSEFA VALCÁRCEL, 44

28027-MADRID

Índice de contenidos

CONTROL DEL DOCUMENTO

Título:	Política de Seguridad de la DGT		
Autor:	GI DGT Área de Seguridad		
Versión:	3.0	Fecha Versión:	22/02/2024
Aprobado por:	Director de la DGT. Las revisiones: el Comité de Seguridad	Fecha Aprobación	09/04/2024
Confidencialidad:	Este documento es propiedad de la DGT. Prohibida su copia o reproducción, tanto total como parcial, sin el consentimiento expreso del propietario.		

CONTROL DE VERSIONES

Versión	Fecha	Modificado por	Descripción
1.0	27/10/2016	GI DGT Área de Seguridad	Versión inicial.
1.1	13/11/2019	GI DGT Área de Seguridad	Verificación de responsabilidades conforme ENS
1.2	15/11/2019	GI DGT Área de Seguridad	Se añaden precisiones menores
1.3	19/11/2019	GI DGT Área de Seguridad	Se añade nuevos responsables de la información a tenor de lo establecido en la PSI del Ministerio del Interior.
2	02/12/2019	GI DGT Área de Seguridad	Comprobación de funciones de los roles acorde a la PSI del Ministerio del Interior.
2.1	07/02/2020	GI DGT Área de Seguridad	Se alimentan campos de referencia inicial relativos a la aprobación, ámbito, revisión, y misión.
2.2	27/02/2020	GI DGT Área de Seguridad	Se suprime y se ubica el Anexo Gobernanza a otro documento como Guía.
2.3	28/02/2020	GI DGT Área de Seguridad	Inclusión de la elevación del presente documento a la GI DGT Área de Seguridad Comisión

			Ministerial de Administración Digital
2.4	18/05/2020	GI DGT Área de Seguridad	Se adecua a la plantilla de la SMO
2.5	10/09/2020	GI DGT Área de Seguridad	Se añaden precisiones menores
2.6	11/09/2020	GI DGT Área de Seguridad	Se añaden precisiones menores
2.7	16/09/2020	GI DGT Área de Seguridad	Aprobación de la PSI.
2.8	14/07/2022	GI DGT Área de Seguridad	Revisión debido a la entrada en vigor del RD 311/2022 (nuevo Esquema Nacional de Seguridad) y tras observaciones a partes de texto efectuadas por el DPD de la DGT
2.9	15/02/2023	GI DGT Área de Seguridad	Escalada y puesta en conocimiento su revisión en el Comité de Seguridad celebrado en fecha 15/02/2023 Y envío posteriormente de la PSI al Director de la DGT para su firma
3.0	22/02/2024	GI DGT Área de Seguridad	Modificado a efectos de SGSI, y cambios menores para cumplir con el ENS.

1. Aprobación y entrada en vigor

El Comité de Seguridad de la Información de este Organismo resolvió aprobar la revisión de la "**Política de Seguridad de la Información**" de la Dirección General de Tráfico.

El presente documento que ha sido elaborado por el Área de Arquitectura, Innovación y Seguridad establece las directrices generales para el uso adecuado de los recursos de tratamiento de información que la Dirección General de Tráfico pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior, entrará en vigor inmediatamente después de su publicación por parte de la DGT. Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de este documento. Por tanto, esta Política de Seguridad de la Información es efectiva desde la fecha arriba indicada y hasta que sea remplazada por una nueva Política.

2. Revisión y evaluación

La gestión de esta política corresponde al Responsable de Seguridad, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Responsable de Seguridad revisará la presente política, en adecuación a las modificaciones del ENS, y legislación relacionada que se someterá, de haber modificaciones, a su posterior aprobación por el Comité de la DGT.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento a través de los medios establecidos a tal fin en la DGT.

3. Ámbito y alcance

La política de Seguridad se aplica a todos los sistemas TIC, y a todos los miembros de la DGT, y por tanto debe ser cumplida y observada por todo el personal, tanto interno como externo, con acceso a la información y a los sistemas de información.

4. Introducción

La Política de Seguridad de la Información es un documento de alto nivel que define lo que significa "seguridad de la información" en una organización.

La Política de Seguridad de la Información se elabora en cumplimiento de la exigencia del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), que en

su Capítulo III concretamente en el artículo 12 establece la obligación para las Administraciones Públicas de disponer de una Política de Seguridad e indica los requisitos mínimos que debe cumplir.

La Ley que regula el Procedimiento Administrativo Común de las Administraciones Públicas y el Régimen Jurídico del Sector Público, consolidan el derecho de los ciudadanos a comunicarse con las Administraciones mediante medios electrónicos. En concreto la segunda de estas leyes, contempla el ENS como norma a seguir al objeto de establecer la política de seguridad en la utilización de medios electrónicos.

Los tres grandes objetivos del ENS son: en primer lugar, alinear el ENS con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital. En segundo lugar, introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios. En tercer lugar, facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

La DGT hace uso de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos institucionales. En consecuencia, estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución y con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que la organización y su personal debe aplicar las medidas mínimas de seguridad exigidas por el ENS, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Por tanto, 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 y reaccionando con presteza a los incidentes.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Los 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 TIC.

Esta Política de Seguridad es conforme con la Orden, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio del Interior (o referida también en este documento como PSI del Ministerio del Interior).

La organización debe estar preparada para contemplar acciones de prevención, detección, respuesta y conservación de amenazas, vulnerabilidades e incidentes de acuerdo al artículo 8 del ENS.

4.1. Prevención

La organización 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 debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

4.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el artículo 9 del ENS.

4.3. Respuesta

La organización debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

4.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, el organismo debe desarrollar planes de continuidad de negocio y actividades de recuperación de cara a evitar degradaciones y garantizar una prestación adecuada de los servicios del Organismo a través de los sistemas de información.

5. Misión

La normativa que regula el Tráfico, Circulación de Vehículos a Motor y Seguridad Vial tiene como objetivo fundamental la reducción de las víctimas de los accidentes de tráfico y velar por la Seguridad Vial en todos los ámbitos. Por ende, a lo anterior, la misión de la DGT es satisfacer las necesidades ciudadanas mediante el cumplimiento de sus tres objetivos primordiales y permanentes: disminuir el número de víctimas y de accidentes de tráfico, garantizar la movilidad a través de una adecuada gestión del tráfico y proveer la gestión de todos los trámites asociados a la gestión de la circulación.

Por tanto, la misión de la DGT consiste en ejercer las competencias del Ministerio del Interior sobre el Organismo Autónomo Jefatura Central de Tráfico, teniendo como centro referencial de sus actuaciones al ciudadano. Para ello, la DGT desarrolla acciones tendentes a la mejora del comportamiento y formación de los usuarios de las vías, a la reducción de los accidentes de tráfico y del número de víctimas; a promover la movilidad segura y la prestación eficiente de servicios administrativos.

5.1. Objetivos generales en materia de seguridad de la información

Como soporte y apoyo a los objetivos operativos mencionados anteriormente, la Política de Seguridad de la Información de la DGT establece los siguientes objetivos generales en materia de seguridad de la información:

- Contribuir desde la gestión de la seguridad de la información al cumplimiento de la misión y objetivos establecidos por la DGT.
- Implementar las medidas de control necesarias que garanticen el cumplimiento de los requisitos legales 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.
- Asegurar que los servicios se prestan tanto de manera preventiva como reactiva ante posibles incidentes de seguridad.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad, y trazabilidad de la información.
- Proteger los activos de información de la DGT, así como la infraestructura tecnológica 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 de la DGT, para la difusión y consolidación de la cultura de la seguridad.

5.2. Objetivos específicos en materia de seguridad de la información

Los objetivos de seguridad específicos de la información son las necesidades que la organización identifica para satisfacer y asegurar la integridad, confidencialidad, disponibilidad, accesibilidad, trazabilidad y autenticación de la información y de los datos propios y de terceros.

Los objetivos de seguridad de la información son también el criterio con el que se fijan indicadores de cumplimiento del Sistema o los que miden la efectividad de los controles y de los procesos de Seguridad de la Información.

En el Anexo I del presente documento, se desarrollan dichos objetivos.

6. Marco normativo

Para la elaboración del presente documento se ha tenido en cuenta la legislación aplicable al Organismo en materia de Tecnologías de la Información, que queda recogida en un registro dispuesto al efecto (REG-006 Registro del Marco Legal Regulatorio), el cual se mantiene actualizado según señala el correspondiente procedimiento de gestión de requisitos legales.

7. Principios básicos.

La política de seguridad de la información se desarrolla con carácter general de acuerdo con los siguientes principios:

1. **Principio de confidencialidad:** se deberá garantizar que los activos sean accesibles únicamente para aquellas personas expresamente autorizadas para ello

2. **Principio de integridad y actualización del sistema:** se deberá asegurar que la información con la que se trabaja sea completa y precisa, y se incidirá en la exactitud tanto de su contenido como de los procesos involucrados.

3. **Principio de disponibilidad, resiliencia y continuidad:** se garantizará la prestación continuada de los servicios y la recuperación inmediata ante posibles contingencias, mediante medidas de recuperación orientadas a la restauración de los servicios y de la información asociada. Se debe procurar que los activos estén disponibles cuando lo requieran las personas autorizadas para acceder a ellos.

4. **Principio de autenticidad:** se deberá garantizar que la información se intercambie con los interlocutores idóneos y que los servicios se acrediten correctamente.

5. **Principio de trazabilidad:** se deberá garantizar el seguimiento de las operaciones efectuadas sobre la información y los servicios que lo requieran, registrándose la actividad de los usuarios.

6. **Seguridad integral:** la seguridad es considerada como parte de la operativa habitual y como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. Además, está presente y aplicándose desde el diseño inicial de los sistemas de información.

7. **Principio de gestión del riesgo:** gestionar la seguridad de la información consiste en analizar los riesgos, establecer medidas de seguridad adecuadas, eficaces y proporcionadas e incluir la corrección y mejora continuas que lleven a que la organización sea cada vez más preventiva que reactiva frente a los incidentes de seguridad. Se deben minimizar los riesgos hasta niveles aceptables y buscar el equilibrio entre las medidas de seguridad y la naturaleza de la información.

8. **Principio de prevención, reacción y recuperación:** se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir, detección, corrección de fraudes, incumplimientos o incidentes relacionados con la seguridad, así como de protección de las instalaciones de la compañía y a la plataforma tecnológica comprendida en el alcance.

9. **Principio de mejora y reevaluación continua:** se revisará, de manera recurrente, el grado de eficacia de los controles de seguridad implantados en la organización para aumentar la capacidad de adaptación a la constante evolución de los riesgos y del entorno tecnológico.

10. **Principio de proporcionalidad en coste:** la implantación de medidas que mitiguen los riesgos de seguridad de los activos deberá hacerse dentro del marco presupuestario previsto a tal efecto y siempre buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el presupuesto previsto.

11. **Principio de concienciación y formación:** se articularán programas de formación, sensibilización y concienciación para las personas usuarias en materia de seguridad de la

información, debidamente apoyados en las políticas corporativas y con un acomodado proceso de seguimiento y actualización.

8. Organización de la seguridad

En concordancia con las Políticas de Seguridad de rango jerárquico superior al presente documento, el Anexo II del ENS, y las Guías CCN–STIC elaboradas por el Centro Criptológico Nacional que desarrollan el ENS, se estableció por medio del presente documento el Grupo de Trabajo para la Seguridad de la Información (en adelante, GTSI) a través del Comité de Seguridad de la información de la DGT.

La composición final del GTSI se comunicará a la Secretaría del Comité Superior para la Seguridad de la Información para su traslado a la Comisión Ministerial de Administración Digital, en el plazo máximo de un mes desde su constitución.

7.1. Comité de la Seguridad de la Información. Funciones y responsabilidades.

El Comité de Seguridad de la Información coordina la seguridad de la información en la DGT, estará liderado por el Responsable de la Seguridad (de la Información) y formado por representantes de otras áreas del Organismo afectadas.

Es la máxima autoridad en la organización respecto a las decisiones de seguridad que afecten a los sistemas que manejan información o prestan algún servicio.

Las funciones indicadas en la PSI del Ministerio del Interior al Comité Superior para la Seguridad de la Información del Ministerio del Interior (o CSSI) las asume un GTSI de cada Centro Directivo dependiente del Ministerio del Interior, que se constituirá a través del Comité de Seguridad de la Información de la DGT siendo sus funciones conformes a las señaladas en la Orden que regula la PSI del Ministerio del Interior, marcándose dentro de sus competencias las que siguen:

- Redactar y aprobar el desarrollo normativo de segundo nivel de la presente política (o en adelante, PSI de la DGT).
- Divulgación de la política y normativa de seguridad de la Organización.
- Velar e impulsar el cumplimiento de la PSI de la DGT y de su desarrollo normativo.
- Aprobación de documentos de correspondencia de responsables en su ámbito competencial, detallados de acuerdo a la normativa en vigor en materia de seguridad y privacidad.
- Aprobación de los planes de mejora de la seguridad en su ámbito de competencias, de acuerdo a los presupuestos disponibles anualmente.
- Informar sobre el estado de las principales variables de seguridad de sus sistemas de información, para la elaboración de un perfil general del estado de seguridad del Ministerio.
- Promover la mejora continua en la gestión de la seguridad de la información en su ámbito de competencias.
- Impulsar la formación y concienciación en su ámbito de actuación.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no se tenga suficiente autoridad para decidir.

La composición final y funcionamiento del GTSI constituido a través del Comité de Seguridad de la Información de la DGT será determinada por el titular del Centro Directivo de entre los funcionarios de carrera adscritos al mismo adecuándose a la estructura del Centro Directivo.

El Comité de Seguridad de la Información de la DGT estará compuesto, por los siguientes miembros, funcionarios de carrera adscritos a la DGT:

a) Responsable de la Información.
b) Responsable del Servicio.
c) Responsable de la Seguridad.
d) Responsable de Sistemas.

Se podrán designar uno o varios Responsables de la Información, uno o varios Responsables de los Servicios, y uno o varios Responsables de Sistemas, de acuerdo a la Organización de la DGT, siendo los mismos titulares de las Unidades Administrativas competentes en la gestión de la información, los servicios y los sistemas informáticos, respectivamente. Dichas funciones serán encomendadas a personal funcionario de la correspondiente Unidad Administrativa.

La designación del Responsable de la Seguridad en la DGT la realizará el Director de la DGT. Este nombramiento será coherente con las estructuras organizativas existentes en relación con la Seguridad de la Información y acorde con las funciones que desempeñan en su puesto de trabajo habitual.

El Responsable de la Seguridad en la DGT será miembro del Grupo de Trabajo de Responsables de Seguridad del Ministerio de Interior conforme a lo indicado en la Orden INT/424/2019, de 10 de abril.

Las competencias y responsabilidades del Responsable de la Información y del Responsable del Servicio de acuerdo a la normativa vigente son indelegables, salvo los casos establecidos por la PSI del Ministerio del Interior como la posibilidad de delegar la aceptación de los riesgos derivados de un análisis de riesgos, así como su seguimiento y control (como así se establece en el artículo 15.2 de la Orden INT/424/2019).

De igual modo, podrá coincidir en la misma persona u órgano las Responsabilidades de la Información y del Servicio. La diferenciación tendrá lugar cuando el servicio maneja información de distintas procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.

Atendiendo a estos criterios, se concreta el nombramiento de cada miembro de la siguiente forma:

- **Responsable de la Información, y Responsable del Servicio:** serán las personas designadas por las diferentes Unidades de Negocio de la DGT.
- **Responsable del Sistema:** recae en el Jefe de Área de Operaciones y Servicios Digitales y, Jefe de Servicio de Gestión de Movilidad y Tecnologías, cada uno en su ámbito de actuación.
- **Responsable de Seguridad** para todos los servicios que da al ciudadano y/u otros organismos de manera electrónica la responsabilidad recae en el titular de la Secretaría General de la DGT quien delega en dos Responsables de Seguridad Delegados: el/la titular de Gerencia de Informática y, el/la titular de la Subdirección General de Gestión de la Movilidad y Tecnologías, cada uno de sus ámbitos de actuación.

El Responsable de Seguridad queda igualmente incluido en el marco de las obligaciones que establece el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Dentro del Comité de la DGT, el Delegado de Protección de Datos de la DGT (en adelante, DPD) participará, con voz, pero sin voto en las reuniones que se establezcan 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. Si bien, cualquier asunto que se sometiese a votación se hará constar en acta el parecer del DPD.

De igual modo el DPD queda integrado en el Grupo de Trabajo de los Delegados de Protección de Datos del Ministerio del Interior para las reuniones que este pueda convocar.

7.2. Roles, funciones y responsabilidades

La DGT establece las figuras enumeradas en el apartado anterior con objeto de dar respuesta a las necesidades en materia de seguridad de la información, en consonancia con los preceptos marcados por el ENS, la LOPDGDD, las Guías CCN–STIC elaboradas por el Centro Criptológico Nacional (CCN), y la PSI del Ministerio del Interior.

DGT cumpliendo con el principio de seguridad según artículo 11 del Real Decreto 311/2022, de 3 de mayo, mantiene las siguientes funciones como excluyentes:

- Responsable de Seguridad
- Responsable del Sistema.

Responsable de la Información

Conforme a los artículos 13 y 41 del Real Decreto 311/2022 de 3 de mayo, el Responsable de la Información tiene la potestad de establecer los requisitos de la información tratada o, en terminología de la Guía CCN-STIC 801, la potestad de determinar los niveles de seguridad de la información.

El Responsable de la Información en este organismo son las personas designadas por las diferentes Unidades de Negocio de la DGT.

Serán funciones del Responsable de la Información, dentro de su ámbito de actuación, las siguientes:

- Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información.
- Son los encargados, junto a los Responsables del Servicio y contando con la participación del Responsable de la Seguridad, de realizar los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar.
- Son los responsables de aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos.
- Para la determinación de los niveles de seguridad de la información, el Responsable de la Información solicitará informe del Responsable de la Seguridad.

Se establece más en detalle en la “Guía para la Gobernanza de la seguridad de la información de la DGT” las actuaciones que ha de seguir el Responsable de la Información.

Responsable del Servicio

Conforme al artículo 13 del Real Decreto 311/2022 de 3 de mayo, el Responsable del Servicio es quien tiene la potestad de establecer los requisitos de los servicios prestados, o en terminología de la Guía CCN-STIC 801, es el encargado de determinar los niveles de seguridad del servicio en cada dimensión de seguridad, dentro del marco establecido en el Anexo I del Real Decreto 311/2022 de 3 de mayo.

El Responsable del Servicio en este organismo son las personas designadas por las diferentes Unidades de Negocio de la DGT.

Serán funciones del Responsable del Servicio, dentro de su ámbito de actuación, las siguientes:

- Determinar los niveles de seguridad del servicio, valorando los impactos de los incidentes que afecten a la seguridad del servicio.
- Son los encargados, junto a los Responsables de la Información y contando con la participación del Responsable de la Seguridad, de realizar los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar propuestas por el Responsable de Seguridad.

- Son los responsables de aceptar los riesgos residuales respecto de los servicios calculados en el análisis de riesgos.
- Para la determinación de los niveles de seguridad del servicio, el Responsable del Servicio solicitará informe del Responsable de la Seguridad.

Se establece más en detalle en la "Guía para la Gobernanza de la seguridad de la información de la DGT" las actuaciones que ha de seguir el Responsable del Servicio.

Responsable de Seguridad

Conforme al artículo 13 del Real Decreto 311/2022 de 3 de mayo, el responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

Teniendo en cuenta la casuística en cuanto a la organización de la DGT desde el punto de vista del derecho administrativo, y dada la distribución, separación física de los elementos y ámbitos de competencia diferenciados se establecen las responsabilidades correspondientes al Responsable de Seguridad sobre el/la titular de la **Secretaría General de la DGT** quien delega sus funciones en **dos Responsables de Seguridad Delegados**: **el/la titular de Gerencia de Informática y el/la titular de la Subdirección General de Gestión de la Movilidad y Tecnologías**, cada uno de sus ámbitos particulares de actuación.

Las principales responsabilidades de esta figura son las siguientes:

- Establecer medidas de seguridad adecuadas y eficaces.
- Coordinar a los diferentes Responsables -de la Información, del Servicio, y de Sistemas- en su labor de valoración de las dimensiones de seguridad de las informaciones y, de los servicios y determinar la categoría de los sistemas según lo establecido en el Anexo I del ENS y en base a la valoración de las dimensiones de los activos de información y, servicios facilitadas por los diferentes Responsables de Información y de Servicio.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en su ámbito de responsabilidad.
- Realizar o promover las auditorias operativas periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad de la Información.
- Promover la formación y concienciación del Servicio de Tecnologías de la Información y las Comunicaciones dentro de su ámbito de responsabilidad y elaborar planes de concienciación y formación.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Promover, analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Elaborar la normativa de seguridad.
- Aprobar los procedimientos operativos de seguridad.
- Realizar el seguimiento y control del estado de seguridad del sistema de información.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Supervisar el registro (o inventario) de activos.

Además se añadirán las siguientes responsabilidades

- Desarrollar las directrices, estrategias y objetivos dictados por el Comité de Seguridad de la Información de la DGT (o GTSI de la DGT).
- Proveer de asesoramiento y apoyo a el Comité de Seguridad de la Información de la DGT.
- Elaborar informes periódicos de seguridad para el Comité de Seguridad de la Información de la DGT que incluyan los incidentes más relevantes de cada período.

De igual modo, en base a lo establecido en el Real Decreto que regula la seguridad de las redes y sistemas de información, el Responsable de Seguridad podrá desplegar las siguientes funciones:

1. Elaborar y proponer las políticas, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que pudieran afectar a la DGT.
2. Desarrollar las políticas, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
3. Elaborar el documento de Declaración de Aplicabilidad.
4. Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
5. Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan en la normativa anteriormente mencionada.
6. Notificar a la autoridad competente sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
7. Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.

Se establece más en detalle en la “Guía para la Gobernanza de la seguridad de la información de la DGT” las actuaciones que ha de seguir el Responsable de Seguridad.

Responsables del Sistema

Conforme al artículo 13 del Real Decreto 311/2022 de 3 de mayo, el responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

Su potestad y funciones están indicadas en el artículo 13 de la PSI del Ministerio del Interior. Es la persona que tiene la responsabilidad de desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

El Responsable del Sistema de la DGT recae en el Jefe de Área de Operaciones y Servicios Digitales y, Jefe de Servicio de Gestión de Movilidad y Tecnologías, cada uno en su ámbito de actuación.

De acuerdo al marco regulatorio vigente, sus principales responsabilidades son las siguientes:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Mantener el inventario de todos los activos que constituyen los sistemas.
- Validar la existencia de autorizaciones previas al paso de nuevos elementos o cambios al entorno de producción.

- Implantar las medidas de seguridad aprobadas y cerciorarse de que las medidas específicas de seguridad se integran adecuadamente dentro del marco general de seguridad.
- Monitorizar periódicamente el estado de seguridad de los sistemas.
- Facilitar y supervisar el acceso de los auditores a los sistemas de información para permitir su labor de auditoría en el marco del ENS.
- Supervisar el proceso formal de autorizaciones al menos en las siguientes situaciones:
    - Entrada de equipos en producción
    - Entrada de aplicaciones en producción.
    - Establecimiento de enlaces de comunicación con otros sistemas.
    - Utilización de soportes de información.
- Para los sistemas de información bajo su responsabilidad deberá realizar el estudio de previo para determinar las necesidades de procesamiento, almacenamiento, medios, instalaciones y personal.
- En caso de servicios prestados por sistemas externos, deberá supervisar el cumplimiento de los acuerdos de servicios acordados.
- Participar en la creación, mantenimiento y prueba del Plan de Continuidad de Negocio.
- Posibilidad de acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y del Responsable de la Seguridad, antes de ser ejecutada.

Véase también la “Guía para la Gobernanza de la seguridad de la información de la DGT” las actuaciones que ha de seguir el Responsable del Sistema.

7.3 Procedimiento de designación.

La designación de los Responsables identificados en esta Política, se realizará en un Anexo sobre la misma. Asimismo, la designación será realizada por el Dirección General de Tráfico y comunicada a las partes afectadas Dirección General de Tráfico.

Los roles de seguridad serán revisados, al menos cada cuatro años, o en caso de que exista una vacante. De existir vacante, la misma deberá ser cubierta en el plazo de un mes, siguiendo el mismo procedimiento.

8 Datos de carácter personal

La DGT trata datos de carácter personal. El Registro de las Actividades de Tratamiento de la organización establecido por los responsables del tratamiento y regulado en el artículo 30 del RGPD recoge la información sobre los datos de los tratamientos efectuados en el organismo.

Todos los sistemas de información de la DGT se ajustarán a los niveles de seguridad requeridos por la normativa en base a la naturaleza y finalidad de los datos de carácter personal y a las medidas de protección técnicas y organizativa requeridas según la legislación vigente.

8.1. Protección de datos de carácter personal: la política de privacidad

En el ámbito de la DGT la garantía de la protección de datos de carácter personal de las actividades de tratamiento es un objetivo compartido por todas las unidades del departamento que se rige por los siguientes principios:

- Licitud, lealtad y transparencia.

- Limitación de la finalidad.
- Minimización de datos.
- Exactitud.
- Limitación del plazo de conservación.
- Integridad y confidencialidad.
- Responsabilidad proactiva.

Para su consecución se establecen las siguientes directrices:

- Estructura organizativa: En el ámbito de la DGT se nombra un DPD que asume, en su ámbito de competencias, las funciones recogidas en el artículo 39 del RGPD. La actuación del DPD se regirá por el principio de independencia, por lo que no recibirán ninguna instrucción en lo que respecta al desempeño de sus funciones. Podrán estar asistidos por grupos de trabajo integrados por representantes de las unidades administrativas de su ámbito de actuación.
- Actividades de tratamiento: Se entiende por tratamiento cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- De acuerdo con el RGPD, y en especial con lo dispuesto en su artículo 17 de la PSI del Ministerio del Interior, el responsable del tratamiento es el titular de la Unidad Administrativa que determine los fines y medios del tratamiento; con carácter general, se corresponde con el titular de la unidad en que se produzca la operación sobre los datos; en los casos en que no se corresponda la definición legal del responsable del tratamiento con el titular de la unidad en que se produzca la operación sobre los datos o haya varias unidades en las que se produzca la operación de los datos, el titular del centro directivo determinará el responsable del tratamiento, para lo cual puede ser asesorado por parte del DPD.
- Para todos aquellos tratamientos de datos que procesen datos de carácter personal que se realicen en el Ministerio del Interior, los responsables de tratamiento deberán proporcionar la información necesaria para elaborar un Registro con sus Actividades de Tratamiento. El DPD dará instrucciones sobre la herramienta y el apoyo necesario para el mantenimiento del citado registro, cuyo contenido deberá corresponderse con la establecida en el artículo 30 del Reglamento general de protección de datos, incluyendo también su base legal.
- Cláusulas informativas: Para garantizar la adecuación permanente de las cláusulas informativas en materia de privacidad, los responsables de tratamiento deberán verificar el cumplimiento continuo de la inclusión de cláusulas informativas sobre el tratamiento de datos personales conforme a los artículos 13 y14 del RGPD, en especial en el momento previo a la recogida de datos personales, tanto en formularios en papel como en medios electrónicos.
- Procedimientos de relación entre las agencias de control, DPD, responsables de tratamiento y ciudadanos: Los ciudadanos pueden ejercitar sus derechos directamente a los responsables de tratamiento, ante el DPD o incluso directamente ante una Autoridad de Control, como por ejemplo, la Agencia Española de Protección de Datos. Los responsables de tratamiento responderán a las peticiones, pudiendo actuar el DPD correspondiente como intermediario con el ciudadano y con otras administraciones, así como llevando la interlocución con las autoridades de control.
- Gestión de riesgos de privacidad: La gestión de riesgos de privacidad se alineará con el análisis de riesgos de la seguridad. El DPD podrá, a petición del responsable del tratamiento, proporcionar asesoramiento y herramientas específicas tanto para esta gestión de riesgos, como para la realización de evaluaciones de impacto en la privacidad para los tratamientos, en especial los de alto riesgo.

- Revisión jurídica de los contratos, acuerdos y convenios con encargados de tratamiento: El DPD proporcionará modelos de cláusulas tipo y asesoramiento para la adecuación de contratos, acuerdos y convenios que incluyan el tratamiento de datos personales.
- Procedimiento de comunicación de brechas de seguridad: El DPD definirá los protocolos correspondientes, coordinados con los responsables de seguridad, para la comunicación de brechas de seguridad que afecten a información con datos de carácter personal.
- Procedimiento de privacidad desde el diseño: El DPD definirá y difundirá un procedimiento de privacidad desde el diseño que tendrá por objetivo el introducir un protocolo dentro del ciclo de vida del desarrollo y mantenimiento de sistemas de información que garantice que se tienen en cuenta las exigencias de seguridad derivadas del manejo de datos personales.
- Auditorías de privacidad y revisión continúa de las medidas de privacidad: El DPD fomentará procesos de auditoría periódica encaminados a la mejora continua del cumplimiento normativo en materia de protección de datos y a la implantación de las medidas correctoras necesarias para mejorar la seguridad de los datos personales.
- Actuaciones de formación y concienciación: El DPD realizará una planificación de actuaciones periódicas de formación y concienciación al personal en materia de privacidad. Asimismo, se impulsará la formación en materia de gestión documental y archivo.

En relación con los sistemas de información que, para soportar la prestación de servicios de administración electrónica, manejen datos de carácter personal, prevalecerán las mayores exigencias contenidas en la normativa de protección de datos en vigor que afecte al sistema de información concreto.

9. Concienciación y formación

El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de la DGT, y a todas las actividades, de acuerdo al principio de Seguridad como proceso integral recogido en el artículo 5 del RD 311/2022, así como la articulación de medios necesarios para que todas las personas que intervengan en los procesos y los responsables jerárquicos tengan sensibilidad respecto de los riesgos que corren. Para ello, se desarrollará una Plan de Formación y Concienciación de la Seguridad a tal efecto.

10. Gestión de riesgos

El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos, deberá realizarse al menos una vez al año. Y excepcionalmente:

- 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 riesgo, el Comité de Seguridad de la Información de la DGT podría establecer una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información de la DGT dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Se propone como metodología a utilizar Magerit para la elaboración de los Análisis de Riesgos, siguiendo las recomendaciones establecidas por el CCN.

11. Desarrollo de la Política de Seguridad de la Información

Esta Política de Seguridad se desarrollará y/complementará por medio de la normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la Intranet Corporativa.

12. Documentación de Seguridad

El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollará en tres niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

- Primer nivel normativo: documentos que ofrecen un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégicos establecidos por los equipos gerenciales de la organización. Siendo la presente Política de Seguridad de Información el documento nodriza del que emanan el resto de políticas o normas.
- Segundo nivel normativo: normativa de segundo nivel, que recoge el detalle de las actuaciones de la normativa de primer nivel, así como la consecución de acciones necearías para el desarrollo de las mismas. Consiste en el conjunto de tareas detalladas y específicas para entornos, sistemas o aplicaciones que normalmente, aportan un mayor grado de detalle de los objetivos marcados en una política.
- Tercer nivel normativo: compuesta por los siguientes tipos (jerárquicamente al mismo nivel e independientes entre sí), entre los que destacan Procedimientos Operativos de Seguridad, Instrucciones técnicas, Guías e Informes, entre otros.
- Todo ello sin perjuicio, de que exista otro tipo de documentación, no contemplada dentro de los apartados anteriores (por ejemplo, evidencias), y que no forme parte de la jerarquía anteriormente descrita.

En caso de que alguno de los documentos anteriores, aplique a un ámbito concreto de los Responsables de Seguridad Delegados, y cuyo alcance no sea el ámbito global de la DGT, podrán ser aprobados por el Responsable de Seguridad Delegado correspondiente.

Además de los documentos citados, la documentación de seguridad del sistema podrá contar, bajo criterio del Responsable de Seguridad correspondiente, con otros documentos de carácter no vinculante: informes, registros, evidencias electrónicas, guías, etc.

Cada Responsable de Seguridad deberá mantener la documentación de seguridad actualizada y organizada, y gestionar los mecanismos de acceso a la misma.

El Comité de Seguridad de la Información de la DGT establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en todo el ámbito de aplicación de la presente política.

13. Obligaciones del personal

Todos los miembros de la DGT tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y, la Normativa de Seguridad, siendo responsabilidad del Comité de la DGT disponer los medios necesarios para que la información llegue a los interesados o afectados.

Se deberá mantener informados en materia de seguridad TIC a todos los miembros del Organismo, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida que la necesiten para realizar su trabajo.

14. Terceras partes

Cuando la DGT preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos actores indicados en la organización de la seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la DGT utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta política de Seguridad y, de la Normativa de Seguridad que ataña a dichos servicios e información.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

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