Política de seguridad de la información de Arriva

Propietarios de la política:

Departamento legal y TIC de Arriva en España

Fecha de entrada en vigor:

01 de agosto de 2024

Fecha de revisión:

1 de Julio de 2025

Área de Negocio del autor:

Área Legal/TIC

Fecha de aprobación por Dirección General

20 de mayo de 2024

1 Introducción

La presente Política de Seguridad de la Información se elabora en cumplimiento de la ISO/IEC 27001:2022 y conforme a lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, siguiendo las indicaciones de la guía actualizada CCN-STIC-805 del Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI).

2 Alcance

Esta política se aplica a todos los sistemas TIC de Arriva y a todos los miembros de la organización, sin excepciones. Es decir, Los Sistema de Información que dan soporte a los procesos de tratamiento de datos de usuarios por atención al cliente, de terceros por siniestros, de trabajadores para gestión de personal, para la organización y la gestión operativa para la prestación del servicio de transporte regular, según el documento de categorización del sistema vigente.

3 Misión y objetivos

Arriva depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos como Organización. 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 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 Arriva y su personal deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, 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.

Todas las áreas 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 de TIC.

Las áreas deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 7 del ENS.

La Política de Seguridad establece las directrices y principios establecidos por Arriva, para garantizar la protección de la información, así como el cumplimiento de los objetivos de seguridad definidos, asegurando así la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad del sistema de información y por supuesto, garantizando el cumplimiento de todas las obligaciones legales aplicables.

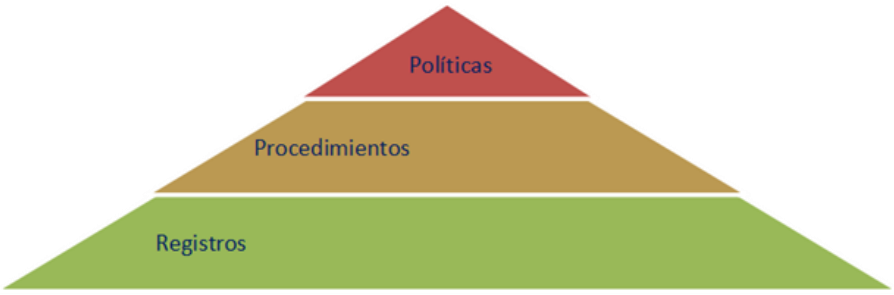
La Dirección de Arriva, consciente de la importancia de la seguridad de la información en el ámbito laboral y de los servicios de transporte que presta, asume y dispone los siguientes compromisos con respecto al Sistema de Gestión de Seguridad de la Información:

- Asegurarse que se establecen objetivos de seguridad de la información, siempre alineados con la estrategia de la empresa.
- Asegurarse que los requisitos de seguridad se integran en los procesos de la organización.
- Asegurar los recursos necesarios para el sistema de gestión de seguridad de la información.
- Comunicar la importancia de una gestión de la seguridad de la información eficaz y conforme con los requisitos del sistema de gestión de seguridad de la información.
- Asegurarse que el sistema de gestión de seguridad de la información consigue los resultados previstos.
- Dirigir y apoyar a las personas, para contribuir a la eficacia del sistema de gestión de seguridad de la información.
- Promover la mejora continua del sistema de gestión.
- Y apoyar los roles pertinentes para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

Para ello, la Dirección asegurará que el personal de Arriva cumple con las normativas, políticas, procedimientos e instrucciones relativas a la seguridad de la información.

Mediante el desarrollo de su Sistema de Gestión de Seguridad de la Información, Arriva pretende garantizar los siguientes objetivos de seguridad:

- Asegurar la confidencialidad, integridad, disponibilidad autenticidad y trazabilidad de la información.
- Cumplir todos los requisitos legales aplicables.
- Tener un plan de continuidad que permita recuperar los procesos y actividades ante un incidente, en el menor tiempo posible.
- Formar y concienciar a todos los empleados en materia de seguridad de la información.
- Satisfacer las expectativas y necesidades en materia de seguridad de clientes, empleados, proveedores, usuarios y demás partes interesadas.
- Gestionar adecuadamente todas las incidencias ocurridas.
- Informar a todos los empleados de sus funciones y obligaciones de seguridad, que son de obligado cumplimiento.
- Mejorar de forma continua el Sistema de gestión y, por ende, la seguridad de la información de la organización
- Estructurar nuestro sistema de gestión de forma que sea fácil de comprender. Nuestro sistema de gestión tiene la siguiente estructura:



Para asegurar el correcto desempeño del Sistema de Gestión de Seguridad de la Información y cumplir con los objetivos y requisitos establecidos, la dirección de Arriva ha designado al responsable del sistema de gestión y a los miembros del Comité de Seguridad que velarán por el cumplimiento de las directrices marcadas por la presente política.

3.1 Prevención

Arriva 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.
- Identificar si un atacante remoto podría penetrar las defensas.
- Determinar el impacto de una violación de seguridad.

3.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben 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 donde las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. El sistema debe disponer de una estrategia de protección constituida por múltiples capas de seguridad, para cuando una de las capas falle permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el sistema.

Las líneas de defensa estarán constituidas por medidas de naturaleza organizativa, física y lógica.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

3.3 Respuesta

El Comité de Seguridad de la información:

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

3.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

4 Marco normativo

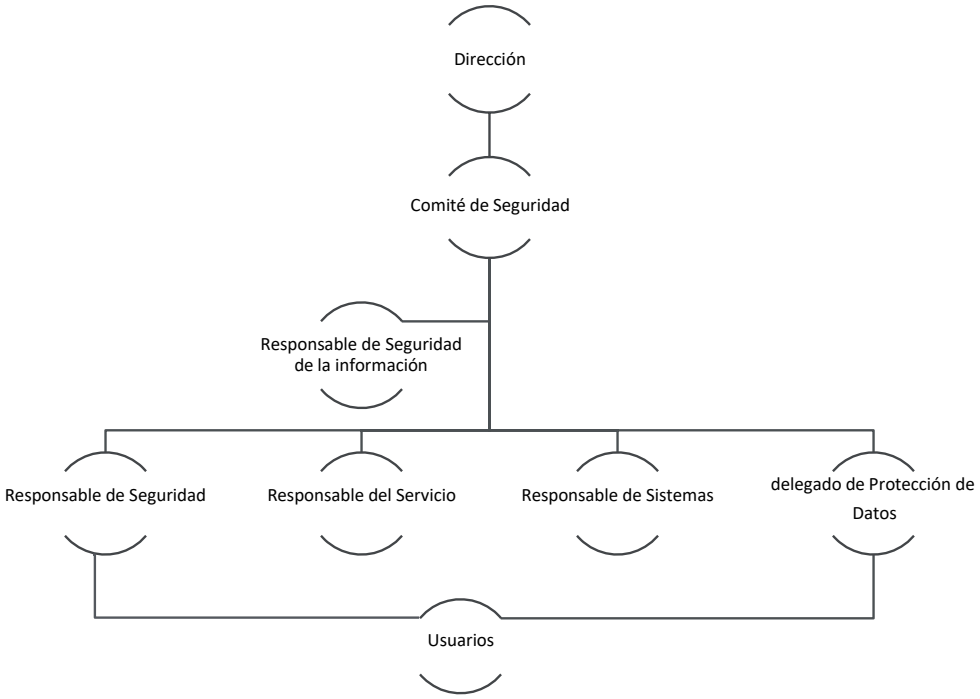
Según la legislación vigente, Arriva se encuentra sujeto a la siguiente normativa en materia de seguridad de la información:

- 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 anterior 95/46/CE (Reglamento general de protección de datos).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- UNE-EN ISO/IEC 27001 es idéntica a la norma internacional ISO/IEC 27001Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI).
- UNE-EN ISO/IEC 27002 que es igual que las normas internacionales ISO/IEC 27002 Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal de Protección de Datos Personales y garantía de los derechos digitales
- Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.
- LO 1/1996 de Protección Jurídica del Menor
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Guías de las series 400, 500 y 800 del CCN-CERT.

Arriva cumple con la legislación citada y con todos sus requisitos.

5 Organización de la seguridad

Se toma como referencia la Guía de Seguridad de las TIC (CCN-STIC 402) Organización y Gestión para la seguridad de los sistemas TIC y la Guía de Seguridad de las TIC (CCN-STIC 801) Esquema Nacional de Seguridad Responsabilidades y Funciones.



5.1 Comité: Funciones y responsabilidades

El Comité de Seguridad coordina la seguridad de la información en Arriva.

La Dirección es responsable de que la organización alcance sus objetivos a corto, mediano y largo plazo. Debe respaldar explícita y notoriamente las actividades de la Seguridad de las TIC en la organización. Expresa sus inquietudes al Comité de Gestión de Seguridad de la Información a través del responsable de la Información. Aprueba la Política de Seguridad de la Información.

El Comité de Seguridad de la Información estará formado por el responsable de Seguridad de la información, El responsable de Seguridad, El responsable del servicio y el responsable del sistema.

Este comité se responsabiliza de alinear todas las actividades de la organización en materia de seguridad de la información.

El **Comité de Seguridad de la Información** reportará a: La Dirección.

El **Comité de Seguridad de la Información** tendrá las siguientes funciones:

- Revisión de la Política de Seguridad de la Información y de las responsabilidades principales y propuesta de aprobación al Órgano de Gobierno.
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinadas a garantizar la Seguridad de dichos activos.
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
  - Principales incidencias en la Seguridad de la Información.
  - Elaboración y actualización de planes de continuidad.
  - Cumplimiento y difusión de las Políticas de Seguridad.

Los miembros del comité de seguridad de la información son:

Responsable de Seguridad: Jésica Criado.

Responsable del Sistema de información: Ignacio Santalla.

Responsable de Servicio: Ricardo Díaz.

Responsable de la información: Ismael Cuevas.

Miembro del comité: Bartolomé del Castillo.

DPO interno: Patricia Romero.

5.2 Roles: funciones y responsabilidades

Los diferentes roles junto con sus respectivas funciones y responsabilidades están reflejados en la siguiente tabla:

Roles y funciones del Comité de Seguridad	
Rol	**Funciones**
Responsable de la Información	• Determinar los requisitos de la información tratada.
Responsable del Servicio	• Determinar los requisitos de los servicios prestados.

Responsable de Seguridad	• Determinar las medidas y políticas a aplicar en todo momento para garantizar los requisitos de seguridad de la información y los servicios.
Delegado de Protección de Datos	• Cumplimiento de la gestión de los datos personales y cumplimiento de la legalidad.
Responsable del Sistema	• Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el responsable de la Seguridad.

5.3 Procedimiento de designación

El responsable de Seguridad de la Información será nombrado por a propuesta del Comité de Seguridad de la información. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

Es función de Comité de Gestión de Seguridad de la Información de la entidad designar:

- El responsable de la Seguridad debe reportar directamente al responsable de la Información y al Comité de Seguridad de la Información.
- El responsable del Sistema, en materia de seguridad, reportará al responsable de la Seguridad. El Departamento responsable de un servicio que se preste electrónicamente designará al responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

5.4 Política de seguridad de la información

Será misión del Comité de Seguridad de la información la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta. La Política será aprobada por la Dirección General de Arriva y difundida para que la conozcan todas las partes afectadas.

6 Datos de carácter personal

Arriva trata datos de carácter personal. Se dispone de un registro de actividades de tratamiento y responsables correspondientes, al que tendrán acceso sólo las personas autorizadas. Todos los sistemas de información de Arriva se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en las políticas de seguridad de la información.

7 Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.

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

8 Desarrollo de la política de seguridad de la información

Esta Política de Seguridad de la Información complementa las políticas de seguridad de Arriva en diferentes materias:

- Políticas del Grupo Arriva:
  - Cyber Security and Information Assurance Policy
  - Business Information Systems Policy
  - Data Protection Policy
  - Acceptable Use Policy)
- Política de uso y disposición de las TIC.
- Aviso Legal y Políticas de privacidad (web).
- Política de seguridad de la información para proveedores.

Esta Política se desarrollará por medio de 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 para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible para todas las partes interesadas en la web www.arriva.es y de manera interna a los trabajadores en SharePoint en las carpetas de 01_Sistemas de gestión/01_Políticas. Además, se realizará una comunicación formal de la misma a todos los miembros de la empresa que tengan correo corporativo y se realizará la publicación de esta en el Portal del Empleado para el resto de los empleados.

9 Obligaciones del personal

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

Todos los miembros de Arriva atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año dentro del Annual Refresher Training del Corporate Confidence de Arriva. Se establecerá un programa de concienciación continua para atender a todos los miembros de Arriva, 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 en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

10 Terceras partes

Cuando Arriva 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 del respectivo Comité de Gestión de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Arriva 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 atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la 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, 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.