itsDUERO

Política de Seguridad

Índice

Aprobación

ELABORADO POR	REVISADO POR	APROBADO POR
Responsable de Seguridad	Responsable del Sistema	Comité de Seguridad

1. Política de Seguridad

La Política de Seguridad de ITS DUERO S.L. nace de la preocupación por parte de la Dirección de garantizar la plena satisfacción de las partes interesadas, de la gestión del servicio ofrecido a los clientes, así como la gestión de la seguridad de sus sistemas de información.

La Dirección de la organización enfoca la Seguridad de la Información, como un sistema para prestar servicios que satisfagan las necesidades del cliente, teniendo en cuenta los requisitos de la actividad de la organización, así como los requisitos legales, reglamentarios o contractuales. Todos los procesos internos y externos quedan adscritos y afectos a la presente política o cuantas políticas transversales se desarrollen para dar cumplimiento a la misma.

La Política de Seguridad tiene por objeto proteger los activos de información del sistema de información de la organización, así como los activos de información de nuestros clientes con los que exista un acuerdo contractual, ante cualquier amenaza, sea interna o externa, deliberada o accidental. Se busca 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 urgencia a los incidentes para recuperarse lo antes posible y minimizar el impacto.

La Seguridad de la Información está implícita en cada uno de los puntos de esta política, e integrada en los procesos de negocio como herramienta clave para conseguir los objetivos de negocio de la organización. Esta política queda alineada plenamente con los objetivos de negocio e integrada en la estrategia de la organización.

ITS DUERO S.L. tiene implantado, y mejora continuamente, un Sistema de Gestión de la Seguridad de la Información acorde con al Esquema Nacional de Seguridad.

La Política de Seguridad tiene vigencia desde la aprobación por la Dirección y mientras no se apruebe una posterior, se mantendrá vigente. La Política es comunicada y puesta a disposición de todos los afectados, tanto internos como externos.

Toda violación de la presente política o aquellas que la desarrollen, de las normas y procedimientos, será considerado por el procedimiento disciplinario, incluyéndose proveedores y colaboradores externos que serán tramitados por su procedimiento oportuno.

2. Alcance

La Política de Seguridad es de aplicación sobre todo el personal de la organización, incluyendo sus contratistas y el personal contratado temporalmente; afecta a cualquier tipo de información, tanto la que sea propiedad de la organización como la que procede de clientes, con independencia del soportes o medio en el que se encuentre, tipología o categoría; y aplica a cualquier activo de información propiedad de la organización que afecte al sistema.

3. Compromisos de la Dirección

El Director General de ITS DUERO S.L. está comprometido con el desarrollo e implementación del Sistema de Gestión de la Seguridad de la Información y con la mejora continua de su eficacia.

El Director General es el Responsable del Comité de Seguridad, y el resto de los responsables y trabajadores de la organización están comprometidos con la seguridad, además de por sus cargos, por formar parte del Comité de Seguridad, y ser así parte activa del mismo.

El Director General:

- Comunica a la organización la importancia de satisfacer tanto los requisitos del cliente como los de seguridad, del servicio, los legales, reglamentarios, y las obligaciones contractuales.
- Establece y comunica el alcance del SGSI.
- Define y comunica la Política de Seguridad, normas y procedimientos.
- Comunica la Política de Seguridad y la importancia de cumplir con ella a clientes y a proveedores (contrato de confidencialidad).
- Asegura el establecimiento y la comunicación de los objetivos de seguridad de la Información.
- Lleva a cabo las revisiones por la Dirección anuales.
- Dirige las revisiones del SGSI.
- Vela por que se realicen las auditorías internas del SGSI, anualmente.
- Asegura que se revisan los resultados de las auditorías para identificar oportunidades de mejora.
- Asegura la provisión y disponibilidad de recursos.
- Asegura que se gestionan y se evalúan los riesgos de seguridad de la información, a intervalos planificados.
- Define el enfoque a tomar para la gestión de los riesgos de seguridad de la información y los criterios para asumir los riesgos.
- Aprueba los niveles de riesgo aceptables para la organización.
- Establece roles y responsabilidades en materia de seguridad.
- Determina las cuestiones externas e internas que son pertinentes para el propósito de la organización y su dirección estratégica.

El compromiso de la Dirección está reflejado en la presente política.

4. Objetivos

Los objetivos del Sistema de Gestión de la Seguridad de la Información (SGSI) de la organización son:

- Mantener una gestión adecuada del SGSI de acuerdo con los estándares de seguridad y las buenas prácticas del sector, llevando a cabo todo esto de manera que se aseguren ventajas competitivas para la organización.
- Proteger la información interna relacionada con la prestación de los servicios, considerando las dimensiones:
    - Confidencialidad para asegurar que la información solo sea accedida por aquellos que cuenten con la autorización respectiva. Toda la información se protegerá de manera que no se pondrá a disposición, ni se revelará a individuos, entidades o procesos, no autorizados previamente.
    - Integridad para preservar la veracidad y completitud de la información y los métodos de procesamiento. Toda la información se protegerá de manera que se podrá asegurar que no ha sido alterado de manera no autorizada. La alteración será entendida en todos sus contextos, es decir, la creación, modificación o eliminación.
    - Disponibilidad para asegurar que los usuarios autorizados tienen acceso a la información y los procesos, sistemas y redes que la soportan, cuando se requiera. La información será accesible a aquellos usuarios o procesos que la requieran y cuando lo requieran. Será principio básico de la organización, la restricción de accesos al mínimo necesario.
    - Trazabilidad para asegurar que queda constancia fehaciente del uso del servicio y del acceso a los datos, es decir, que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. Toda acción desarrollada en el sistema o sobre la información, puede ser imputada a su autor, en cualquier fase de ciclo de vida o en cualquier fase de proceso.
    - Autenticidad para asegurar que quien accede al servicio es realmente quien se cree y garantizar la fuente de la que proceden los datos. Toda información puede ser asignada a una fuente o todo autor puede ser contrastado y acreditar su identidad sin lugar a dudas.
- Establecer anualmente objetivos específicos en relación a la Seguridad de la Información, que garanticen la mejora continua del SGSI, siendo estos consistentes con los presentes objetivos.
- Desarrollar un proceso de análisis del riesgo y, de acuerdo a su resultado, implementar las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables, según los criterios establecidos.
- Establecer los medios necesarios para garantizar la continuidad del negocio de la organización.
- Cumplir con los requisitos del negocio, las obligaciones legales y las obligaciones contractuales de seguridad.
- Asegurar que los activos de la organización solo sean utilizados por usuarios autorizados en el ejercicio de sus funciones, sus perfiles definidos o según asignaciones extraordinarias.
- Establecer y difundir los roles y responsabilidades relacionados con la Seguridad de la Información.
- Sensibilizar y concienciar de manera estable y permanente a todo el personal de la organización en cuanto a la seguridad de la información.
- Fomentar y mantener el buen nombre de la organización en relación a los servicios desarrollados, saber y respuesta activa (reactiva y proactiva) ante incidentes de seguridad, mantenimiento la imagen y reputación.
- Reflejar en la Declaración de Aplicabilidad del ENS las medidas de seguridad y dimensiones definidos en el Esquema Nacional de Seguridad.
- Sancionar cualquier violación a esta política, así como a cualquier política o procedimiento del SGSI.

5. Legislación aplicable y requisitos contractuales

Las obligaciones legales aplicables a la organización relativas a la seguridad de la información se reflejan en:

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad	Toda la organización.
Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.	
Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.	
Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.	
Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.	
Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD).	Toda la organización: tratamiento de datos de carácter personal.
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.	
Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE)	Actividades comerciales en internet de la organización.
Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.	
Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza	Firma electrónica
Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 (eIDAS), relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior	
Ley Orgánica 10/1195, de 23 de noviembre, del Código penal.	Toda la organización.
Copyright – Derecho de autor. Real decreto 1/1196 Derechos de autor y propiedad intelectual. Ley 17/2001 Derechos de marcas nombres comerciales.	Licencias software, nombres comerciales.
Ley 38/2003, de 17 de noviembre, General de Subvenciones.	Toda la organización: subvenciones otorgadas por la Administracion pública
Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.	Toda la organización: legislación laboral.

Real Decreto-ley 32/2021, de 28 de diciembre, de medidas urgentes para la reforma laboral, la garantía de la estabilidad en el empleo y la transformación del mercado de trabajo.	
Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social.	
Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social	
Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales.	
Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres.	
Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual.	
Real Decreto 901/2020, de 13 de octubre, por el que se regulan los planes de igualdad y su registro y se modifica el Real Decreto 713/2010, de 28 mayo, sobre registro y depósito de convenios y acuerdos colectivos de trabajo.	
Real Decreto 902/2020, de 13 de octubre, de igualdad retributiva entre mujeres y hombres.	
Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación	
Ley 39/1999, de 5 de noviembre, para promover la conciliación de la vida familiar y laboral de las personas trabajadoras.	
Ley 10/2021, de 9 de julio, de trabajo a distancia	
Directiva (UE) 2019/1937 del Parlamento Europeo y del consejo de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión “Directiva Whistleblowing”.	
Convenio Colectivo de ámbito provincial del sector de comercio de Soria (Nº Convenio 42000025011981)	Toda la organización: Convenio colectivo

Además, se consideran los requisitos contractuales establecidos en contratos de clientes o proveedores que requieren de requisitos específicos en materia de seguridad.

6. Estructura de seguridad

Se define una estructura para asignar las responsabilidades de seguridad. Esta estructura conformará el **Comité de Seguridad**.

El **Comité de Seguridad** estará formado por:

- **Responsable del Comité de seguridad**: Tiene funciones estratégicas, deberá formular la política del SGSI, establecerá los objetivos del SGSI y velará por su cumplimiento, aprueba roles y responsabilidades en materia de seguridad de la información, comunicará a la organización la importancia de cumplir con los objetivos y la política de seguridad, sus responsabilidades legales y la necesidad de la mejora continua. Proporciona recursos suficientes para crear, implementar, operar, supervisar, mantener y mejorar el SGSI. Decide los criterios y niveles de aceptación del riesgo. Vela por que se realicen las auditorías internas del SGSI, dirigirá

las revisiones del SGSI, y deberá revisar los informes de auditoría, comprobar que se hacen controles periódicos, aprobar mejoras técnicas propuestas, etc.

- **Responsable de Seguridad**: Sus funciones serán: realizar el análisis de riesgos, proponer el nivel de riesgo residual aceptable, evaluar e implantar contramedidas, y revisar y mejorar el SGSI de manera continua. Además, elaborará la Declaración de aplicabilidad, y propondrá al responsable del Comité de Seguridad mejoras técnicas, proponiendo estrategias y solicitando recursos encaminados a conseguir los objetivos de seguridad establecidos. Se encargará de llevar a cabo todas las directrices marcadas por la Dirección en el ámbito de la seguridad de la información.

- **Responsable del Sistema**: Su función será principalmente la de desarrollar, operar y mantener el sistema de Información durante todo su ciclo de vida, sus especificaciones, instalación y verificación de su correcto funcionamiento. Además, se cerciorará de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

Este Comité tendrá comunicación continua con los directores de los diferentes departamentos para desplegar y mantener aquellas medidas que afecten a su área de negocio, así como para recibir información sobre las necesidades de seguridad que se detecten en cada caso.

La renovación de dichos roles y funciones queda renovada de forma automática en cada reunión periódica del Comité de Seguridad. **Se mantendrán reuniones semestrales, convocándose reuniones extraordinarias siempre que se considere necesario para tratar temas de seguridad de la información**. La designación de nuevas funciones, nuevos roles y/o nuevos miembros será realizada por el Responsable del Comité.

Los roles y responsabilidades en relación al SGSI son comunicados a las nuevas incorporaciones y recordados periódicamente a todo el personal de la organización.

7. Documentación de seguridad del sistema

La documentación generada dentro del SGSI es controlada y aprobada por el Comité de Seguridad.

7.1. Información pública

Todo registro, archivo, documento o cualquier dato que se recopila, mantiene, procesa o se encuentra en poder de cualquier trabajador, que no tenga el carácter de confidencial, ni de restringida; y que puede ser distribuida a terceros ajenos a la organización, sin que esto suponga ningún riesgo de escape o fuga de información, de revelación o de modificación no autorizadas. Se incluyen aquí todos los folletos, documentos manuales, informes, newsletters, noticias, etc. que la organización facilita hacia el exterior, y que no requiere un tratamiento de control de seguridad específico. Este tipo de documentación se identificará de manera sencilla por su diseño, que tendrá un objeto publicitario.

En este tipo de información no se encontrarán datos de carácter personal.

7.2. Información interna

La documentación que la organización utiliza para ofrecer sus servicios, está almacenada en soporte digital; y aquella que llega conformada en formato papel es escaneada y almacenada en digital en su carpeta de restringido acceso correspondiente. Si fuera necesario almacenar algún documento en papel: su archivo se realizará de forma responsable y controlada por la persona que maneja dicho documento. Esta información es de acceso restringido para los trabajadores, no pudiendo acceder a ella personal externo no autorizado. El acceso a la documentación estará controlado por los privilegios de acceso de cada trabajador, tanto a nivel lógico como físico.

Se envían correos periódicos de sensibilización y concienciación sobre el buen manejo de la información que cada trabajador utilice; y sobre normas de seguridad a tener en cuenta. Asimismo, toda nueva incorporación es informada sobre dichas normas.

En este tipo de documentación sí se podrán encontrar datos de carácter personal por lo que se requerirá el cumplimiento de lo establecido en los Acuerdos de Confidencialidad y Secreto Profesional correspondientes.

7.3. Información confidencial

Toda aquella documentación en papel que contiene información sensible bien de los trabajadores o bien de los clientes y proveedores, considerada como confidencial queda siempre en manos de los distintos responsables definidos en la tabla anterior de Calificación de la Información y es archivada en el despacho del Responsable de Administración, con acceso controlado y restringido bajo llave.

Asimismo, y para aquellos departamentos que tengan armarios con llave, pueden almacenar los documentos que consideren que, por su contenido, tienen carácter confidencial; quedando la llave exclusivamente bajo la tutela del director de este departamento en cuestión, o del propio trabajador en el caso de tratarse del cajón de su propia mesa.

Toda la información en soporte digital está estructurada y protegida de accesos malintencionados, mediante políticas de acceso por puesto y carpeta que el Responsable del Sistema gestiona, aplicando los privilegios que cada Director de Departamento le comunique. El acceso a la documentación estará controlado por los privilegios de acceso de cada trabajador, tanto a nivel lógico como físico.

En este tipo de documentación sí se podrán encontrar datos de carácter personal por lo que se requerirá el cumplimiento de lo establecido en los Acuerdos de Confidencialidad y Secreto Profesional correspondientes.

8. Principios de seguridad

El SGSI se encuentra enmarcado por los siguientes principios de seguridad:

- Seguridad por defecto.
- Seguridad basada en el liderazgo y en la organización.
- Organización de la Seguridad
- Seguridad basada en procedimientos
- Seguridad gestionada en base al riesgo
- Seguridad considerando incidentes
- Continuidad de los servicios
- Seguridad considerando la gestión de recursos
- Seguridad de áreas y entorno
- Seguridad como requisito legal

8.1. Seguridad por defecto

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La seguridad del sistema contempla los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

Las funciones de operación, administración y registro de actividad son las mínimas necesarias, y se asegura que sólo son accesibles por las personas, o desde localizaciones o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso.

El uso del sistema es sencillo y seguro, de forma que una utilización insegura requiere de un acto consciente por parte del usuario.

Para mantener el proceso de seguridad integral, se realiza una organización de la información en carpetas de acceso restringido, conforme a los principios de protección frente a pérdidas, accesos indebidos, divulgación o uso indebido, deterioro de la información o pérdida de disponibilidad. Cada usuario únicamente accede a la información que requiere para llevar a cabo su actividad.

Se conoce en todo momento el estado de seguridad del sistema o de sus componentes, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les puedan afectar.

8.2. Seguridad basada en el liderazgo y en la organización

La seguridad compromete a todos los miembros de la organización, en base a sus diferentes roles, considerando diferentes responsabilidades.

La Dirección es quien lidera la organización y promueve la cultura de seguridad, asignando los roles requeridos y potenciando la transversalidad de la seguridad en cada proceso desarrollado o servicio a terceros.

La seguridad del sistema es revisada de conformidad a los requisitos, la política y los procedimientos aprobados por la Dirección. Las revisiones son por parte de la Dirección y por revisiones internas o auditorias del sistema. Específicamente la organización y el sistema se pueden someter a procesos de certificación externos, conforme a lo establecido por el Esquema Nacional de Seguridad y cualquier otro estándar de seguridad que le pudiera interesar.

8.3. Organización de la seguridad

Se establece una estructura organizativa en la organización, donde se establecen roles específicos, pero siempre considerando el principio de separación de funciones. Se designan a las personas que ocupan los roles, por periodos anuales, siendo estos renovados automáticamente mientras que la Dirección no establezca una nueva persona para ocupar el cargo.

8.4. Seguridad basada en procedimientos

La seguridad del sistema se documenta mediante procedimientos de operación que son puestos a disposición de los usuarios implicados en el mismo. Los cambios son gestionados, las capacidades del sistema son medidas y controladas y los entornos están separados. Se desarrollan procedimientos de protección del sistema, incluyendo procedimientos de copias y restauración.

Se documentan los acuerdos con proveedores y colaboradores que forman parte del sistema. La cadena de suministro es controlada con relación a los requisitos de seguridad, la prestación de servicios o los cambios de suministradores.

Las redes son gestionadas, incluyendo cuando sea necesario, el cifrado o el control de comunicaciones.

8.5. Seguridad gestionada en base al riesgo

La gestión de riesgos es parte esencial del proceso de seguridad, manteniéndose permanentemente actualizado, bajo el liderazgo de la Dirección.

La gestión de riesgos se realiza por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema de información y la organización, basándose en la metodología MAGERIT v3 y detallada y documentada en el documento correspondiente, permitiendo la repetición de la medición y análisis.

8.6. Seguridad considerando incidentes

El proceso de gestión de incidentes, incluye la detección y notificación de los incidentes de seguridad, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas, especialmente cuando afecta a terceros, y el registro de las actuaciones ejecutadas.

Los incidentes de seguridad permiten la recopilación de evidencias, de manera que se pueda identificar y documentar la recogida, la adquisición y la preservación de la información.

8.7. Continuidad de los servicios

La continuidad forma parte del sistema de gestión, conforme a las necesidades de la organización y los controles establecidos. La organización considera el análisis de impacto y las consecuencias de la información que el mismo muestre.

8.8. Seguridad considerando la gestión de recursos

Todo el personal relacionado con el sistema y con la información, es formado e informado de sus deberes y obligaciones en materia de seguridad, siendo controladas y supervisadas sus acciones.

Cada usuario que accede a la información del sistema está identificado de forma única, de modo que se conoce, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

La responsabilidad es exigible mediante un procedimiento disciplinario**,** que al igual que las pautas de seguridad, conoce previamente el usuario. Este procedimiento está alineado con la normativa laboral.

El usuario con acceso concedido al sistema, pueda o no desarrollar acciones, está sometido a secreto y reserva, aun cuando finalice su relación con la organización. Ningún usuario accede al sistema sin estar previamente informado de este extremo.

8.9. Seguridad de áreas y entorno

La organización previene los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Las áreas pueden ser de control propio o derivadas al propio prestador afectado.

8.10. Seguridad como requisito legal

La Dirección establece como requerimiento de seguridad, el pleno cumplimiento de las obligaciones legales y contractuales, ligadas a la información. Los requisitos son identificados y organizados para su correcta gestión.

Para tener éxito en la Política de Seguridad enunciada, esta Dirección solicita la adhesión y participación de todos a todos los niveles, tanto en sus actuaciones individuales como cuando forman parte de grupos de trabajo, con el fin de establecer y mantener al día un Sistema de Gestión de Seguridad de la Información que asegure la satisfacción de nuestros clientes y la consecución de los Objetivos de Negocio.

9. Datos de carácter personal

ITS DUERO S.L. trata datos de carácter personal de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril (GDPR), y la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD). La organización está cumpliendo con todas las disposiciones del GDPR para el tratamiento de los datos personales de su responsabilidad, y manifiestamente con los principios descritos en el artículo 5 del GDPR, por los cuales son tratados de manera lícita, leal y transparente en relación con el interesado y adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

La organización garantiza que implementa políticas técnicas y organizativas apropiadas para garantizar las medidas de seguridad que establece el artículo 32 GDPR con el fin de proteger los derechos y libertades de los interesados.

Control de cambios del documento

Versión	Fecha	Motivo del cambio
1	02/08/2022	Creación documento.
2	10/01/2023	Aprobación documento.