ARITEX

PSI 5.2 POLÍTICA SEGURIDAD DE LA INFORMACIÓN

Preparado:	**Revisado:**	**Aprobado:**
Xavier Casanovas Chief Information Officer	Comité Seguridad de la Información	Iván Ros Chief Executive Officer **Fecha**: 07/08/2026

PSI 5.2 POLÍTICA SEGURIDAD DE LA INFORMACIÓN

Contenido

1 PRÓLOGO 3
2 REFERENCIAS 3
3 DEFINICIONES 3
4 ALCANCE 4
5 RESPONSABILIDADES Y COMPROMISO 4
6 OBJETIVOS 5
7 AUDITORIA Y CONTROL 6
8 COMUNICACIÓN 6
9 ACTUALIZACIÓN Y REVISIÓN 6
10 CONTROL DE CAMBIOS 7

PSI 5.2 POLÍTICA SEGURIDAD DE LA INFORMACIÓN

1 PRÓLOGO

ARITEX CADING, S.A.U es una empresa especializada en el diseño, fabricación e instalación y puesta en marcha de soluciones industriales automatizadas para, principalmente, los sectores de automoción y aeronáutico, así como construcción, ferrocarril y general industry.

La Dirección de ARITEX CADING, S.A.U. reconoce que la información es un recurso valioso para nuestra organización y, por tanto, debe ser protegida. Esta información puede presentarse en varias formas: impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o medios electrónicos, representada como imágenes o transmitida en conversaciones. La seguridad de la información protege la información de una amplia gama de amenazas para asegurar la continuidad comercial de la empresa, minimizar el daño a la misma y maximizar su productividad.

La Política de Seguridad de la Información de ARITEX CADING S.A.U. parte del compromiso, por parte de la Alta Dirección, de garantizar la plena satisfacción de los grupos de interés de la organización, así como la gestión de la seguridad de sus sistemas de información.

2 REFERENCIAS

El sistema de gestión de seguridad de la información ARITEX CADING S.A.U. sigue el código de prácticas acorde con las normas UNE-ISO/IEC 27001:2022 y TISAX (Trusted Information Security Assessment Exchange), que es un estándar de seguridad impulsado por la VDA, que recoge los requisitos fundamentales de la norma ISO 27001 en seguridad de la información y los adapta a la industria automotriz.

3 DEFINICIONES

1. "**Compañía**" refiere a la sociedad ARITEX CADING S.A.U. y/o cualesquiera de sus sociedades filiales.

2. "**Empleado**" refiere a cualquier persona que esté empleada como aprendiz, empleado permanente,
3. empleado con contrato especial o ejecutivos de cualquier nivel contratados por la Compañía.

4. "**Usuario**" refiere a los empleados, incluyendo personal externo, que en la lista de usuarios autorizados puedan tener una contraseña de acceso y/o una contraseña para acceder a cualquier sistema informático.

5. "**Tecnologías de la Información (TI)**" se refiere a información, noticias, registros, historial, contenido de documentos, programa de computadora, datos de computadora en imágenes, sonidos, marcas o símbolos, ya sea que estén almacenados en un formato que pueda transmitir significado a una persona directamente o mediante herramientas o cualquier equipo.

6. "**Seguridad**" se refiere a cualquier proceso o acción, como prevención, severidad, precaución, cuidado en el uso y mantenimiento de los sistemas informáticos / TI e información confidencial para evitar cualquier intento de acceso del Empleado interno o externo con la intención de robar, destruir e interrumpir dicho sistema que pueda causar daños al negocio.

7. "**Externo**" se refiere al personal de agencias o empresas externas que realizan negocios o brindan servicios que pueden ser otorgados con acceso a TI y a equipos que procesan información de la

Compañía, tales como socios comerciales, recursos subcontratados, proveedores, proveedores de servicios y / o consultores.

4 ALCANCE

Esta Política se aplicará a toda la Compañía. Será vinculante para todo el personal, independientemente de su puesto y cargo. La aplicación de esta Política, en su totalidad o en parte, puede extenderse a cualquier persona física y/o jurídica asociada con la Compañía en cualquier término que no sea una relación laboral, cuando esto sea factible debido a la naturaleza de la relación, y pueda ser apropiado para cumplir con su propósito.

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

En virtud de esta Política, ARITEX podrá desarrollar varios procedimientos e instrucciones para implementar y hacer cumplir las obligaciones asumidas, y adecuarlas a las diferentes leyes y regulaciones locales aplicables al Grupo. Todos los procesos internos y externos quedan adscritos y afectados a la presente política, o a cuantas otras políticas transversales se desarrollen para dar cumplimiento a la misma. La aplicación de esta Política es complementaria a otras normativas internas obligatorias.
Toda violación de la presente política o de aquellas que la desarrollen, de las normas y procedimientos correspondientes, será evaluada, tratada y, en su caso, sancionada de acuerdo con los procedimientos previstos al efecto, incluidos proveedores y colaboradores externos

5 RESPONSABILIDADES Y COMPROMISO

La Alta Dirección de ARITEX CADING S.A.U. está comprometida con el desarrollo e implementación del Sistema de Seguridad de la Información, y con la mejora continua de su eficacia.

El Responsable de Seguridad de la información de ARITEX CADING S.A.U. dirige todo lo relativo a la seguridad de la información en el Sistema Integrado de Gestión (SIG). Asimismo, los demás miembros del equipo directivo de la organización se encuentran comprometidos con el sistema de gestión de seguridad de la información formando parte del Comité de Seguridad de la Información.

La Dirección de ARITEX CADING S.A.U., junto con el Comité de Seguridad de la Información, adquiere como compromiso:

- Dotar de los recursos necesarios y definir las funciones y responsabilidades necesarias para implantar y mantener el proceso de mejora continua de la Gestión de la Seguridad de la Información.
- Comunicar a la organización la importancia de satisfacer tanto los requisitos del cliente como los de seguridad, los legales, reglamentarios, y las obligaciones contractuales.
- Establecer y comunicar el alcance del Sistema de Gestión de Seguridad de la Información.
- Definir y comunicar las políticas, normas y procedimientos de Seguridad de la Información.
- Comunicar la Política de Seguridad y la importancia de cumplir con ella a clientes y a proveedores.
- Asegurar el establecimiento y la comunicación de los objetivos de de seguridad de la Información.
- Llevar a cabo las revisiones por la Dirección anuales.
- Dirigir las revisiones del Sistema de Gestión.
- Velar por que se realicen las auditorías internas del SGSI.
- Asegurar que se revisan los resultados de las auditorías para identificar oportunidades de mejora.
- Asegurar la provisión y disponibilidad de recursos.

- Asegurar que se gestionan y se evalúan los riesgos de seguridad de la información, a intervalos planificados.
- Definir el enfoque a tomar para la gestión de los riesgos de seguridad de la información y los criterios para asumir los riesgos.
- Aprobar los niveles de riesgo aceptables para la organización.
- Establecer roles y responsabilidades en materia de seguridad.
- Determinar las cuestiones externas e internas que son pertinentes para el propósito de la organización y su dirección estratégica.

El compromiso de la Dirección se encuentra reflejado en los siguientes objetivos.

6 OBJETIVOS

Esta Política de Seguridad tiene por objeto proteger los activos de información del sistema de gestión de la información de ARITEX, 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 seguridad de la información y la prestación segura y 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.

Con el fin de garantizar una adecuada gestión de la seguridad de la información, Aritex define los siguientes objetivos para su sistema de gestión de seguridad de la información:

- Mantener una gestión adecuada del Sistema de Gestión 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 de:
    - **Confidencialidad** para asegurar que la información sólo sea accesible a aquellas personas 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 alterada 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. Será principio básico de ARITEX la restricción de accesos al mínimo nivel necesario.
- Establecer anualmente objetivos específicos en relación con la Seguridad de la Información, que garanticen la mejora continua del Sistema de Gestión, siendo estos consistentes con los actuales objetivos.
- Desarrollar un proceso de análisis del riesgo y, de acuerdo con su resultado, implementar las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables.
- 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 ARITEX en cuanto a la seguridad de la información.

- Fomentar y mantener el buen nombre de ARITEX en relación con los servicios desarrollados, y dar una respuesta activa (reactiva y proactiva) ante incidentes de seguridad, manteniendo y mejorando la imagen y reputación.
- Reflejar en la Declaración de Aplicabilidad los objetivos de control definidos, basados en los controles recogidos en el Anexo A de la norma 27001:2022.
- Sancionar cualquier violación a esta política, así como a cualquier política o procedimiento del Sistema de Gestión.

7 AUDITORIA Y CONTROL

ARITEX CADING S.A.U. se reserva expresamente el derecho a tomar, con la debida proporcionalidad, las medidas de seguimiento y control que sean necesarias para establecer el adecuado uso de los Sistemas de Información que pone a disposición de sus empleados, incluyendo la verificación del contenido de las comunicaciones y dispositivos, de acuerdo con las leyes y regulaciones aplicables. El Grupo se someterá a revisiones y controles periódicos y estará sujeto a auditorías internas y externas para evaluar el cumplimiento general de la Política.

Cualquier posible infracción de la Política se determinará en el procedimiento correspondiente, de conformidad con las disposiciones aplicables, sin perjuicio de las responsabilidades legales, incluidas las sanciones en el entorno laboral, que puedan imponerse a la parte infractora.

8 COMUNICACIÓN

Esta Política estará disponible para todos los empleados en Intranet y para todas las partes interesadas de la Compañía en el sitio web corporativo. Asimismo, la Política estará sujeta a las oportunas acciones de divulgación, formación y sensibilización, encaminadas a su plena comprensión e implementación.

9 ACTUALIZACIÓN Y REVISIÓN

Esta política será revisada al menos una vez al año por el Comité de Seguridad de la Información, y actualizada en acuerdo unánime por el Comité de Seguridad de la Información al menos una vez anualmente, en su caso, para adecuarla a los cambios que pueda sufrir la empresa y su modelo de negocio, o que se produzcan en el contexto en el que opera el Grupo, asegurando siempre la efectiva implementación de ésta.

Una vez que la política revisada haya sido aceptada por la Política de Seguridad de la Información, deberá ser aprobada por el Director Ejecutivo de la Compañía.

PSI 5.2 POLÍTICA SEGURIDAD DE LA INFORMACIÓN

10 CONTROL DE CAMBIOS

Rev.	Date (DD.MM.YY)	Change
01	17.06.12	Primera versión.
02	29.05.21	Restructurada, extendida, y algunas secciones actualizadas.
03	13.01.22	Añadidas correcciones para TISAX alcance standard.
04	19.01.22	Versión revisada por Comité Seguridad de la Información.
05	14.11.22	Reformular las responsabilidades del empleado para que inequívocamente se deba seguir la Política de Uso y Control de Recursos Tecnológicos (PSI28.1). Quitar referencia al pie respecto plantilla. Cambio CEO a Ivan Ros y aprobación.
06	06.02.23	Revisión anual por parte del ISC. Aprobación por dirección
07	30.01.24	Simplificación y adecuación de la política. Aprobación por CEO
08	16.06.25	Actualización y revisión política
08	30.09.25	Aprobación por el comité SGSI
09	06.03.26	Revisada y renombrada
10	07.08.26	Revisión y aprobación por Dirección