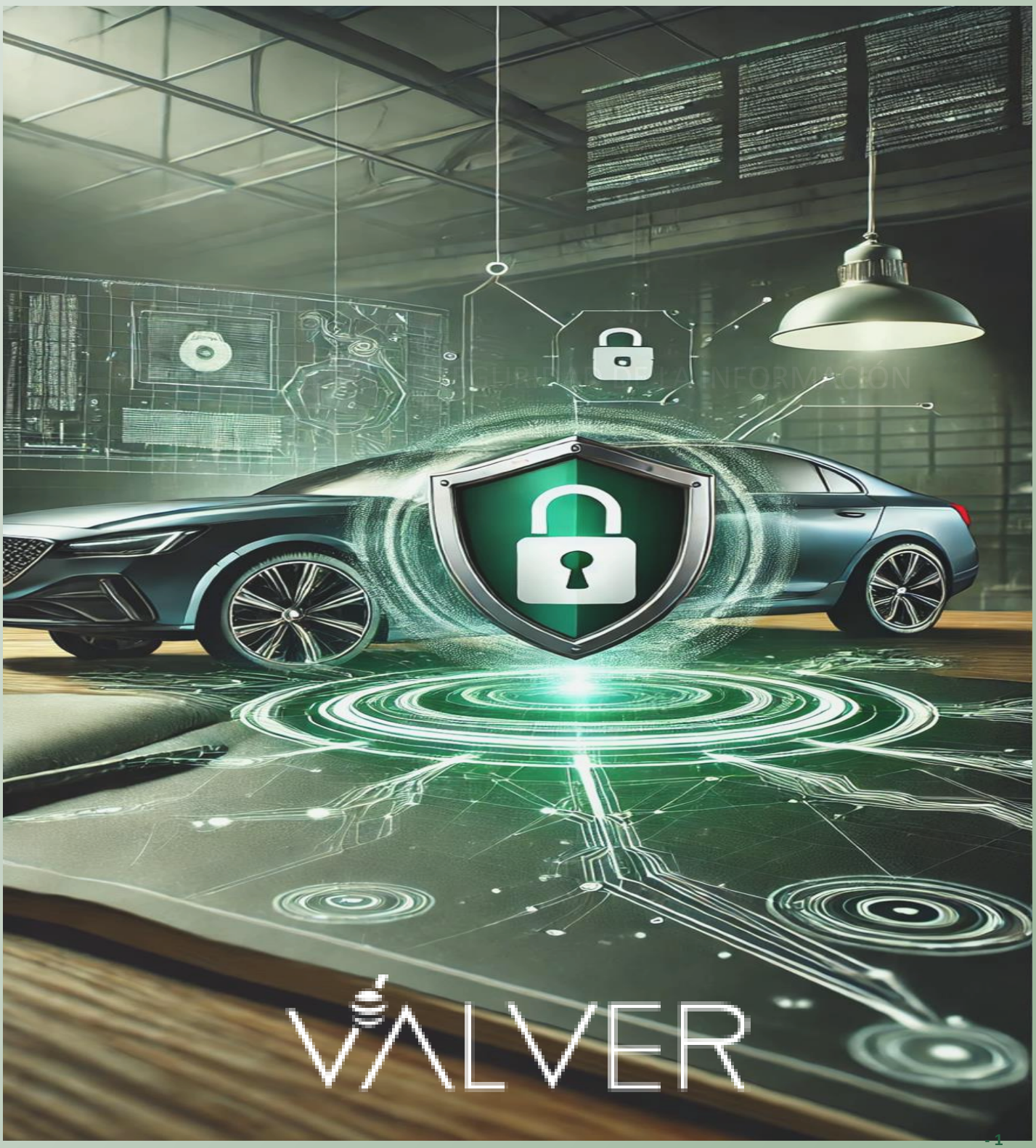
POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN



POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

SEGURIDAD DE LA INFORMACION

Protección de Información Sensible

En la industria automotriz, se maneja una gran cantidad de información sensible, como propiedad intelectual, planos de diseño, datos de fabricación, innovaciones tecnológicas y más. TISAX ayuda a garantizar que esta información esté debidamente protegida contra filtraciones, hackeos o accesos no autorizados.

Cumplimiento de Normas y Regulaciones

TISAX permite a las empresas cumplir con las normativas de seguridad exigidas por sus socios comerciales, especialmente dentro de la industria automotriz europea. Es una forma de estandarizar y simplificar el proceso de auditoría y evaluación para las empresas.

Requisitos de Clientes y OEMs (Fabricantes de Equipos Originales)

Muchas de las grandes empresas automotrices, como Audi, BMW, Daimler y Volkswagen, exigen a sus proveedores la certificación TISAX para asegurar que todos cumplan con las normativas de seguridad. De esta manera, los fabricantes pueden confiar en que los datos sensibles se manejen adecuadamente.

Confianza y Reputación

Obtener una certificación TISAX incrementa la confianza entre los socios comerciales y puede mejorar la reputación de una empresa al demostrar que sus prácticas de seguridad están alineadas con los mejores estándares de la industria..

Estandarización en la Evaluación de Seguridad

TISAX estandariza cómo se evalúan los riesgos y las vulnerabilidades en la seguridad de la información dentro de la cadena de suministro. Esto simplifica los procesos de auditoría, ya que todas las empresas participantes pueden acceder a la misma evaluación y compartir resultados con varios socios comerciales.

Competitividad

Que Valver cuente con la certificación TISAX es, en muchos casos, un requisito para seguir siendo competitivo en la industria automotriz. Sin ella, las empresas pueden verse excluidas de ciertos proyectos o colaboraciones importantes..

En resumen, **TISAX es crucial para garantizar la seguridad de la información en la cadena de suministro automotriz, cumplir con los requisitos de los clientes y mantener la competitividad en un sector altamente regulado.**

ANEXO 3 – Política general de Seguridad de la Información. Certificación Tisax

Consciente de la trascendencia de la seguridad de la información en el contexto actual, VALVER ha impulsado el establecimiento de un Sistema de Gestión de la Seguridad de la Información de acuerdo con los requisitos de la norma VDA-ISA de TISAX basado en la familia de estándares ISO 27000 y con el fin de identificar, evaluar y minimizar los riesgos a los que se expone su información y garantizar el cumplimiento de los objetivos establecidos.

Esta política de seguridad es aplicable a las empresas del grupo de España y Portugal.

Mediante la elaboración, comunicación y mantenimiento de esta política, la Dirección de VALVER. muestra su compromiso de proteger la confidencialidad de la información en la prestación de sus servicios, garantizar su integridad en todos los procesos de tratamiento que lleve a cabo, así como la disponibilidad de los sistemas de información implicados en estos tratamientos.

La presente política se basa en los siguientes principios para garantizar que los sistemas de información y la información que se crea, recopila, almacena y procesa cumple con:

• La seguridad en la gestión de los recursos humanos, antes, durante y al finalizar el empleo.

• La gestión adecuada de los activos que implique la clasificación de la información y la manipulación de los soportes.

• Establecer las medidas oportunas para el tratamiento de los riesgos derivados de la identificación y evaluación de activos.

• El establecimiento de un robusto control de acceso lógico a sus sistemas y aplicaciones, gestionando los permisos y los privilegios de los usuarios.

• La protección de las instalaciones y del entorno físico, mediante el diseño de áreas de trabajo seguras y la seguridad de los equipos.

• La garantía de la seguridad en las operaciones mediante la protección contra el software malicioso, la realización de copias de seguridad, el establecimiento de registros y su supervisión. el control del software en explotación. La gestión de las vulnerabilidades técnicas y la elección de técnicas adecuadas para la auditoría de los Sistemas.

• La seguridad de las comunicaciones, protegiendo las redes y el intercambio de información.

• El aseguramiento de la seguridad en la adquisición y mantenimiento de los sistemas de información, limitando y gestionando el cambio.

• Establecer una metodología de gestión de seguridad de la información clara y eficiente a través de directrices y políticas.

• Garantizar el acceso seguro a la información y con total confianza a los usuarios a través del diseño y operación de una infraestructura de TI y de comunicación de acuerdo con los riesgos actuales de la tecnología.

• Garantizar el correcto estado de las instalaciones y el equipamiento adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa

• La realización de un desarrollo seguro de software, separando los entornos de desarrollo y producción, y realizando las pruebas funcionales de aceptación adecuadas.

• El control de las relaciones con los proveedores, exigiendo de forma contractual el cumplimiento de las medidas de seguridad pertinentes y unos niveles aceptables en la prestación de sus servicios.

• La eficacia en la gestión de los incidentes de seguridad, estableciendo los canales adecuados para su notificación, respuesta y aprendizaje oportuno.

• La realización de un plan de continuidad de negocio que proteja la disponibilidad de los servicios durante una crisis o desastre.

• La Identificación y cumplimiento de la normativa aplicable poniendo especial interés en la propiedad intelectual y en la protección de los datos de carácter personal.

• La revisión de los presentes requerimientos de la seguridad de la información para garantizar el cumplimiento y eficacia de estos.

El Responsable de Seguridad será el responsable directo del mantenimiento de esta política, prestando consejo y guía para su implementación y correcciones ante desviaciones en su cumplimiento. La presente política se hallará siempre alineada con las políticas generales de la compañía y con las que sirvan de marco a otros sistemas de gestión interna, como son las políticas de calidad e IATF.

Todo el personal de la organización tiene el deber de cumplir esta política, para lo cual la Dirección dispone los medios necesarios y recursos suficientes para su cumplimiento, y asume la responsabilidad de comunicarla y mantenerla accesible a todas las partes interesadas.

You name it. We print it

VALVER

VALVER SLU

Parque Empresarial Areas
Rúa 6, Número 39
36711 Tui
Pontevedra (España)

T: +34 986 288 012
E: contact@valvergroup.com

Oct, 2024