

TISAX - Trusted Information Security Assessment Exchange

Ya vivimos en la sociedad de la información: gran parte de nuestras actividades diarias se basan en el almacenamiento, el uso y la transmisión de información. En la automoción, **fabricantes y proveedores comparten a diario datos sensibles** como diseños o prototipos. La información es un activo, tangible o intangible, con un determinado valor para los procesos de negocio de las organizaciones. Por eso **debe protegerse** de forma proporcional a ese valor.

La seguridad de la información debe aplicarse a toda la información, sea cual sea su fuente, tipo, estado o forma, sin confundirla con la seguridad informática. Esta forma parte de aquella, pero la seguridad de la información también abarca el papel, la protección física y los prototipos.

TISAX, el estándar de evaluación de la seguridad de la información del sector de la automoción impulsado por la **VDA**, se basa en el catálogo **VDA ISA**, derivado de la norma **ISO/IEC 27001**. Este catálogo define los controles necesarios para proteger la información según sus dimensiones de seguridad: Confidencialidad, Integridad y Disponibilidad.

TISAX se basa en la gestión de los riesgos: estos se identifican, se evalúan y se tratan según el nivel de protección que requiere la información. Así se adapta a cualquier organización y genera confianza en toda la cadena de suministro.

En esta ficha podrá descargar una práctica presentación en PDF del estándar TISAX

Solicitar **Información**

Autoevaluación **On Line**

Ver video de **Presentación**



Principales **REQUISITOS**

- El LIDERAZGO imprescindible de la alta dirección;
- La CLASIFICACIÓN de la información según su nivel de protección (confidencial, estrictamente confidencial);
- EVALUACIÓN, GESTIÓN y TRATAMIENTO del RIESGO, como elemento clave;
- MEDIDAS ORGANIZATIVAS, TÉCNICAS y LEGALES, para lograr la protección de la información;
- Establecimiento de MECANISMOS DE CONTROL de acceso físico, lógico, control de red y criptográficos;
- PROTECCIÓN DE PROTOTIPOS, componentes y vehículos, en instalaciones, transporte, pruebas y eventos;
- Asegurar la seguridad de la información en la CONEXIÓN CON TERCEROS y en el INTERCAMBIO de información con clientes y proveedores;
- Disponer de CONTRATOS DE CONFIDENCIALIDAD con los empleados;
- Formalización de ACUERDOS CON PROVEEDORES que incluyan requisitos de seguridad;
- Cumplimiento con la LEGISLACIÓN APLICABLE en materia de protección de datos personales;
- USO DE SOFTWARE con licencias;
- GESTIÓN DE INCIDENTES de seguridad de la información y su comunicación a los clientes afectados;
- La importancia de la seguridad de la información debe comunicarse dentro de la organización: la TOMA DE CONCIENCIA Y EL COMPROMISO de todas las personas son imprescindibles para que el sistema funcione;
- Proporcionar la FORMACIÓN necesaria para garantizar la competencia de las personas que realizan tareas relacionadas con la seguridad de la información;
- Garantizar la CONTINUIDAD DEL NEGOCIO, con planes de contingencia y pruebas periódicas.

Ejemplos de **ACCIONES PRÁCTICAS A IMPLEMENTAR**

- Análisis de riesgos de seguridad de la información.
- Clasificación y etiquetado de la información según su nivel de protección.
- Contratos de confidencialidad con empleados y proveedores, según los requisitos de los clientes.
- Acuerdos de prestación de servicio que incluyan requisitos de seguridad.
- Credenciales de acceso a las instalaciones para visitantes.
- Mecanismos que impidan el acceso no autorizado a las áreas seguras: dispositivos biométricos, etc.
- Zonas de seguridad para prototipos, con control de accesos, videovigilancia y prohibición de fotografías.
- Medidas de camuflaje y protección de prototipos durante el transporte, las pruebas y los eventos.
- Sistemas de alimentación ininterrumpida (SAI).
- Control de temperatura en el CPD.
- Uso de software con licencia.
- Planes de continuidad de negocio.
- Planes de prueba: caída del suministro eléctrico, fallo de servidores, fallo de comunicaciones, incendio del edificio, etc.
- Política de gestión de contraseñas y autenticación multifactor.
- Limitación de los usuarios genéricos y de los permisos de administración.
- Restricción de los puertos USB a puestos determinados.
- Antivirus en todos los equipos de la organización, incluidos los dispositivos móviles.
- Firewalls y VPN.
- Control del acceso remoto a la organización, con autenticación segura.
- Filtrado de la navegación web y sistemas de detección de intrusos.
- Copias de seguridad.

Solicitar **Información**

Autoevaluación **On Line**

Ver video de **Presentación**



- Segmentación de redes y conexiones seguras con clientes y proveedores.
- Almacenamiento cifrado de las claves de acceso a sistemas, datos y servicios.
- Certificados digitales y cifrado para el intercambio de información.

*Estas acciones son solo ejemplos y deben adaptarse a la realidad de cada organización y a los objetivos de evaluación TISAX que le exijan sus clientes.

Solicitar **Información**

Autoevaluación **On Line**

Ver video de **Presentación**



Ventajas para **LA ORGANIZACIÓN**

Muchas organizaciones no conocen la información que gestionan, o no saben lo importante que es, hasta que una incidencia les enfrenta a la dura realidad. En la automoción, una fuga de datos de un cliente o de un prototipo puede tener consecuencias muy graves.

Las organizaciones están expuestas a múltiples amenazas (fallos energéticos, malware, fraude, error humano, fallo de equipos, accesos indebidos, desastres naturales, espionaje industrial, …), a las que son más o menos vulnerables y para cuya gestión deben estar preparadas.

Implantar las medidas de seguridad exigidas por TISAX, según el catálogo VDA ISA, permite reducir la probabilidad de que esas amenazas se materialicen y estar preparados para minimizar su impacto si ocurren (pérdidas financieras, multas, pérdida de clientes y de contratos, daños de imagen, interrupción de la producción, costes de recuperación, …).

TISAX nos lleva a establecer las políticas, procedimientos, herramientas informáticas y medidas físicas necesarias para proteger nuestros activos de forma proporcionada, de acuerdo con los niveles de protección que exigen nuestros clientes.

Ventajas para **LOS CLIENTES**

- Acceso a nuevos clientes: facilita trabajar con fabricantes de automóviles (OEM) y proveedores de primer nivel (Tier 1) que exigen TISAX.
- Homologación como proveedor: permite acreditar el cumplimiento de determinados requisitos de seguridad de la información exigidos por clientes del sector.
- Ventaja competitiva: diferencia a la empresa frente a competidores que todavía no han superado la evaluación.
- Acceso a licitaciones y contratos: facilita participar en procesos de contratación donde TISAX constituye un requisito de elegibilidad.
- Reconocimiento internacional: sus resultados pueden ser reconocidos por múltiples organizaciones participantes en el ecosistema TISAX.

Ventajas para **EL MERCADO**

Empresas comprometidas con la seguridad de la información, que garantizan una gestión de la información conforme a las exigencias del sector de la automoción.

Sectores **DE APLICACIÓN**

TISAX está pensado para la industria de la automoción y se aplica a organizaciones de cualquier tamaño que formen parte de su cadena de suministro. Define qué controles de seguridad de la información deben tener según el tipo de información que gestionan.

Solicitar **Información**

Autoevaluación **On Line**

Ver video de **Presentación**



Es especialmente útil para las empresas que manejan información sensible de fabricantes o proveedores del sector, como fabricantes de componentes, ingenierías, empresas de diseño y desarrollo, proveedores de servicios de tecnología, logística o pruebas, o cualquier otra organización que trabaje con prototipos, datos técnicos o datos personales de sus clientes.

Solicitar **Información**

Autoevaluación **On Line**

Ver video de **Presentación**