

Organiza:



Apoyo institucional:



#27CongresoAutomociónAEC

27 Congreso de Calidad en la Automoción 4.0

Barcelona, 20 y 21 de abril de 2023

Automotive EV-olution
Powered by Quality



TISAX

José M^a Moreno
CEO

ÍNDICE

- NECESIDADES
- QUÉ ES TISAX
- PROCESO DE CERTIFICACIÓN





Stephen Hawking
@StephenH



"Creo que los virus informáticos deberían contar como vida. Creo que dice bastante sobre nosotros el hecho de que la única forma de vida que hemos logrado crear sea puramente destructiva. Hemos creado vida basada en nuestra imagen"

11:34 AM · Mar 14, 2018

250.5M Retweets

216.5M Quote Tweets

456.2M Likes



INFORMACIÓN

INFORMACIÓN

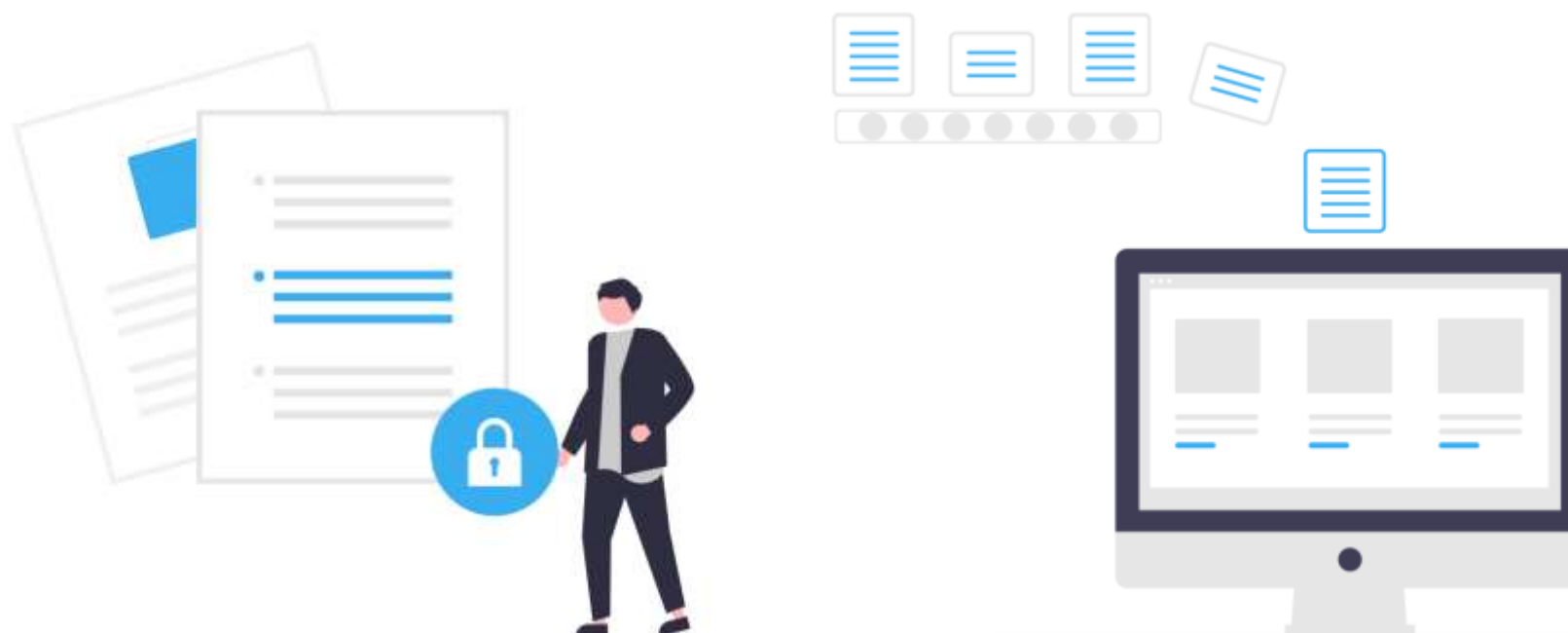
COMUNICACIÓN

CLIENTES

RIESGO

¿QUÉ ES TISAX?

OBJETIVOS



COMUNICACIÓN

INFORMACIÓN

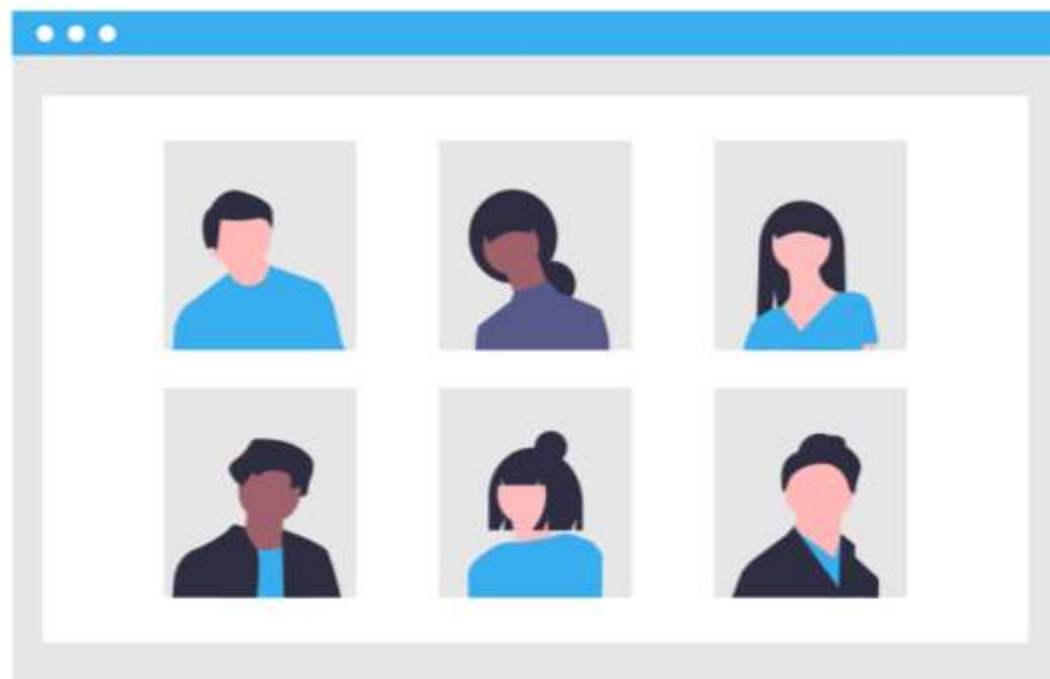
COMUNICACIÓN

CLIENTES

RIESGO

¿QUÉ ES TISAX?

OBJETIVOS



INFORMACIÓN
COMUNICACIÓN

CLIENTES

RIESGO
¿QUÉ ES TISAX?
OBJETIVOS

CLIENTES



INFORMACIÓN
COMUNICACIÓN
CLIENTES

RIESGO

¿QUÉ ES TISAX?
OBJETIVOS

RIESGO



INFORMACIÓN
COMUNICACIÓN
CLIENTES
RIESGO

¿QUÉ ES TISAX?

OBJETIVOS

¿TISAX?



ISO 27001



ESTRATÉGICO

Seguridad de la Información

ANÁLISIS DE
RIESGOS

BUENAS
PRÁCTICAS

PROCEDIMIENTOS



OPERATIVO 27

Seguridad Informática

CONFIGURACIÓN
SEGURA

TÉCNICAS DE
PROTECCIÓN

GESTIÓN DE
INCIDENTES

INFORMACIÓN
COMUNICACIÓN
CLIENTES
RIESGO

¿QUÉ ES TISAX?

OBJETIVOS

OBJETIVOS A CONSEGUIR EN TISAX

27



Establecer un Nivel Común de Seguridad para la Industria de Automoción



Asegurar el Reconocimiento Común de las evaluaciones



Reducir los Costes, Esfuerzos y Complejidad



Asegurar la Comparabilidad y la Calidad de las Evaluaciones



Intercambiar las **Mejores Prácticas** y las **Lecciones Aprendidas**



Cada participante decide a **QUIEN** revelará los **RESULTADOS** y **CON QUÉ** grado de detalle





VS



Enfoque en los Procesos de Seguridad de la Información

Evaluación según Nivel de Madurez

El alcance de la certificación es “FIJO”

Análisis de riesgos predefinido s/VDA-ISA

Obtención de Etiquetas TISAX

Enfoque en el Sistema de Gestión

Evaluación según OK/NOK

El alcance es Personalizable

Análisis de riesgos según la evaluación de las empresas

Obtención de Certificado



SEGUIMIENTO

INTERCAMBIO INFORMACIÓN

6

PLAN ACCIONES

5

AUDITORÍA

4

PREPARACIÓN

3

NECESIDAD

2

1

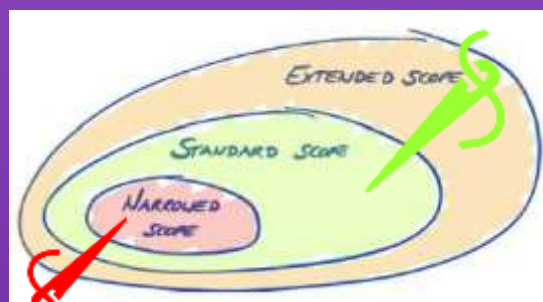
TISAX

PROCESO DE CERTIFICACIÓN

NECESIDAD

- ☐ Aumento de la Concienciación
- ☐ Los participantes activos reciben las primeras informaciones sobre las evaluaciones TISAX

- Un cliente (participante pasivo) solicita una evaluación TISAX o una “etiqueta TISAX” específica al proveedor (participante activo).
- El alcance de la evaluación suele abarcar uno o más procesos (de desarrollo, logística o producción etc).
- Los objetivos de la evaluación dependen de los requisitos de la empresa, el cliente puede solicitar resultados mínimos específicos (etiquetas TISAX).



TISAX

PROCESO DE CERTIFICACIÓN

NECESIDAD

1

NECESIDAD

Assessment method	Assessment level 1 (AL 1)	Assessment level 2 (AL 2)	Assessment level 3 (AL 3)
Self-assessment	Yes	Yes	Yes
Evidences	No	Plausibility check	Thorough verification
Interviews	No	By audio conference ¹⁷	In person, on site
On-site inspection	No	In certain cases ¹⁸	Yes

TISAX

PROCESO DE CERTIFICACIÓN

NECESIDAD

1

- Existen 3 niveles:
 - El nivel inicial o AL1, se asemejaría a un autodiagnóstico. *No es certificable*.
 - En el nivel intermedio o AL2, el auditor solicitará pruebas de los resultados mostrados en la autoevaluación y realizará entrevistas con el personal. *Esto se hará normalmente en remoto*.
 - El nivel más alto, el AL3, implica que el auditor añade más profundidad a las acciones del AL2, y *se realizaría in situ*.

NECESIDAD

No.	TISAX assessment objective	Assessment level (AL)
1.	Information with high protection needs	AL 2
2.	Information with <u>very</u> high protection needs	AL <u>3</u>
3.	Protection of prototype parts and components	AL 3
4.	Protection of prototype vehicles	AL 3
5.	Handling of test vehicles	AL 3
6.	Protection of prototypes during events and film or photo shootings	AL 3
7.	Data protection According to Article 28 ("Processor") of the European General Data Protection Regulation (GDPR)	AL 2
8.	Data protection with <u>special</u> categories of personal data According to Article 28 ("Processor") with special categories of personal data as specified in Article 9 of the European General Data Protection Regulation (GDPR)	AL <u>3</u>

PREPARACIÓN

- ☐ El participante se registra en el portal TISAX
- ☐ Solicitar oferta para el alcance necesario de la evaluación
- ☐ El participante selecciona la entidad de evaluación
- ☐ Se prepara para la auditoría
- ☐ Preparar la documentación (incluida la Autoevaluación VDA ISA)

➤ El participante está de acuerdo con el alcance y la evaluación de TISAX.

➤ El participante se inscribe en la red TISAX y solicita una evaluación con el alcance y los objetivos de evaluación predefinidos.

➤ El participante negocia y firma un contrato con el proveedor de la auditoría.

➤ El participante prepara la auditoría y la documentación (incluida la autoevaluación VDA ISA).

Para obtener más información se puede conseguir a través de este link:

<https://www.vda.de/vda/en/topics/digitization/data/information-security>

TISAX

**PROCESO DE
CERTIFICACIÓN**

PREPARACIÓN

- El formulario VDA ISA contiene “3 catálogos de criterios” o “módulos” (diferentes pestañas del Excel).
- La pestaña “Seguridad de la información” es obligatoria para todas las evaluaciones TISAX.
- Los demás módulos son opcionales. Su aplicabilidad depende de sus objetivos de evaluación.



VDA

Verband der
Automobilindustrie

TISAX
**PROCESO DE
CERTIFICACIÓN**

SEGUIMIENTO

INTERCAMBIO INFORMACIÓN

6

PLAN ACCIONES

5

AUDITORÍA

4

3

PREPARACIÓN

NECESIDAD

2

1

PREPARACIÓN

- En el módulo “Seguridad de la Información” hay un total de 41 controles a cumplir.
- En el módulo “Protección Prototipos” hay un total de 22 controles a cumplir.
- En el módulo “Protección de Datos” hay un total de 4 controles a cumplir.

Las medidas a implementar tiene relación con controles de las normas ISO 27001, ISO 27002, ISO 27017 y aspectos legales del RGPD.

TOTAL DE 67 CONTROLES.



SEGUIMIENTO

INTERCAMBIO INFORMACIÓN

6

PLAN ACCIONES

5

AUDITORÍA

4

3

PREPARACIÓN

NECESIDAD

2

TISAX
**PROCESO DE
CERTIFICACIÓN**

1

PREPARACIÓN

ELEMENTOS DE VDA-ISA 5.1

ACCIONES

SEGUIMIENTO

6

INTERCAMBIO INFORMACIÓN

Maturity Level

CHAPTER

CONTROL QUESTION

REQUIREMENTS

Information Security Assessment Questionary

Sub-Chapter	Sub-Maturity level	Control question	Requirements (Should)	Requirements (Should)	Additional requirements for high protection needs	Additional requirements for very high protection needs	
5.1	5.1.1	Is Policies and Organisation Information Security Policy available?	The organization needs at least one information security policy. This reflects the importance and significance of information security and is adapted to the organization. Additional policies may be appropriate depending on the size and structure of the organization.	The requirements for information security have been determined and documented. • The requirements are aligned to the goals of the organization. • The requirements are based on the organization's management system. • The policy includes objectives and the significance of information security within the organization.	The information security requirements based on the strategy of the organization, legislative and contractual obligations are reflected in the policy.	None	None
5.2	5.2.1	Organisation of Information Security					

OBJECTIVE

ALL PROTECTION NEEDS

HIGH PROTECTION NEEDS

VERY HIGH PROTECTION NEEDS

1. 2. 3.

Welcome Cover Maturity levels Definitions Information Security Prototype Protection Data Protection Results (ISAS)

TISAX

PROCESO DE CERTIFICACIÓN

1

PREPARACIÓN

La VDA ISA proporciona una evaluación de la aplicación basada en un modelo de madurez definido en esta tabla, donde se indica también una breve descripción de los niveles de madurez:

Nivel 0: La aplicación de los requisitos es incompleta. No existe un proceso o el proceso existente no logra los resultados requeridos.

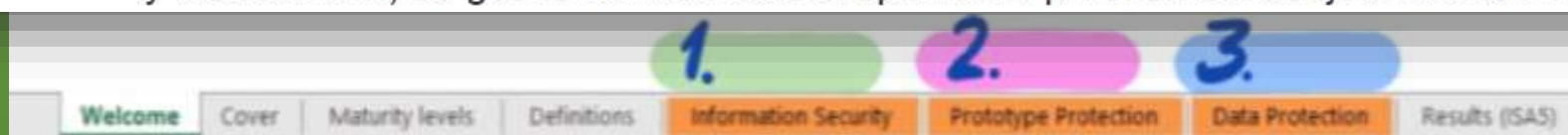
Nivel 1: Se realizan los requisitos necesarios para las respectivas necesidades de protección de la información. Un proceso está en marcha y muestra signos de su funcionamiento. Sin embargo, no está completamente documentado. Por lo tanto, no se puede asegurar su funcionamiento en todo momento.

Nivel 2: Se gestiona el proceso para alcanzar el objetivo. Se documenta y se dispone de evidencias (por ejemplo, documentaciones).

Nivel 3: El proceso está definido, y se definen las dependencias y las vinculaciones con otros procesos internos y externos a la empresa.

Nivel 4: Los requisitos del Nivel 3 y, además, los resultados se miden (por ejemplo, KPI) haciendo que el proceso sea predecible.

Nivel 5: Los requisitos del Nivel 4 y, además, los recursos adicionales (por ejemplo, el personal y las finanzas) se gestionan de manera óptima. El proceso está sujeto a una mejora continua.



AUDITORÍA

- ☐ Reunión inicial
- ☐ Revisión de la documentación por parte del Auditor
- ☐ Auditoría en remoto o in situ (AL2 ó AL3)
- ☐ Entrevistas
- ☐ Reunión de cierre
- ☐ Aclaración de los posibles hallazgos y las próximas acciones

➤ La evaluación inicial de TISAX comienza con una reunión inicial, en la que se determina la fecha de la auditoría y los documentos necesarios (KOM).

➤ Tras una revisión de la documentación (incluida la autoevaluación de la VDA ISA), la evaluación TISAX continúa con una auditoría remota (AL2) o auditoría in situ (AL3), dependiendo del objetivo de la evaluación.

➤ Durante la reunión de cierre, el auditor informa al participante sobre los posibles hallazgos y se aclaran los siguientes pasos (PAC, Informe de seguimiento o de evaluación)

➤ Los primeros resultados suelen estar disponibles en unas pocas semanas (dependiendo del alcance).

AUDITORÍA

PREPARACIÓN

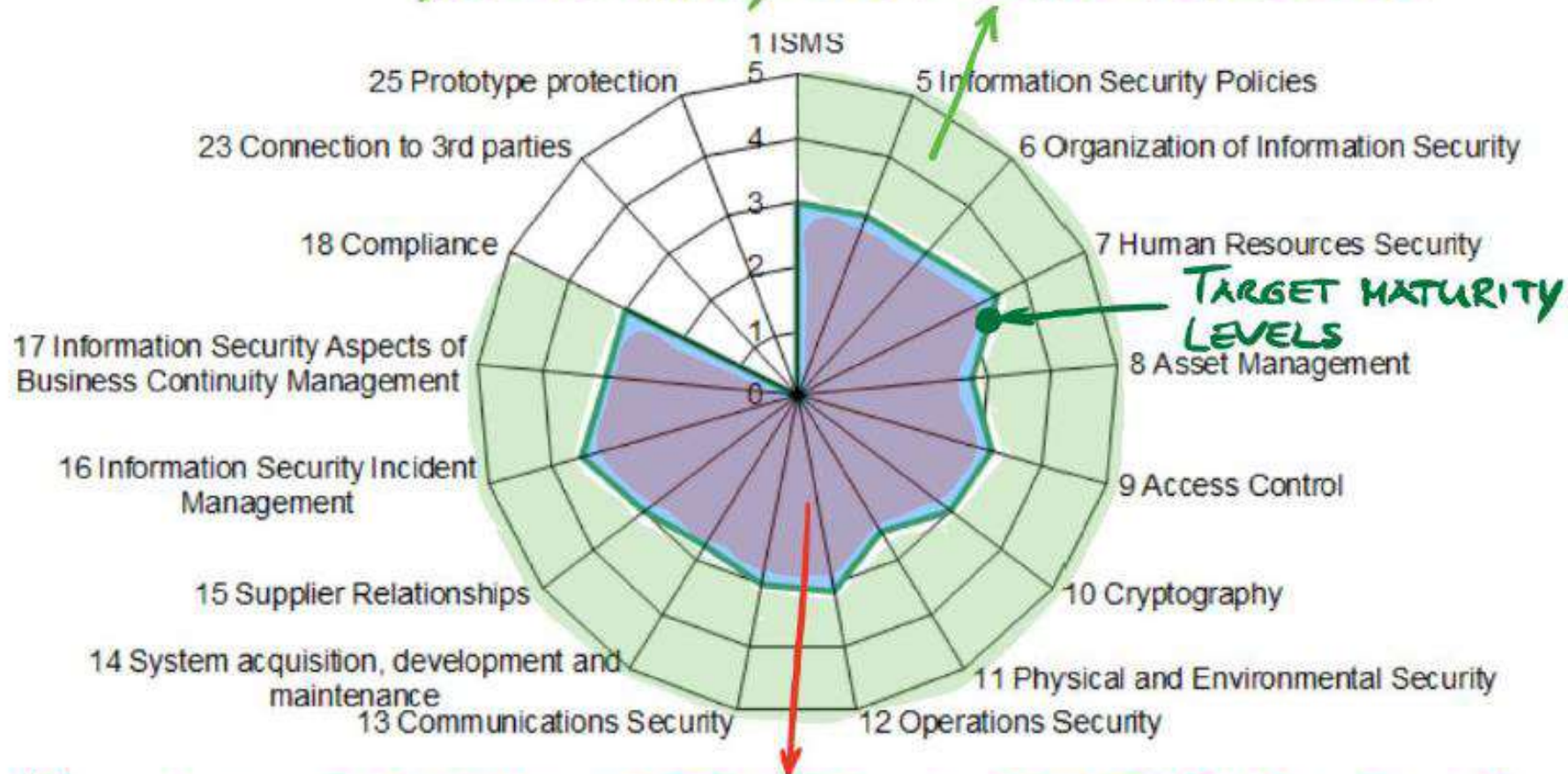
NECESIDAD

TISAX

PROCESO DE CERTIFICACIÓN

AUDITORÍA

YOU ARE READY FOR A TISAX ASSESSMENT



MATURITY LEVELS MAY NOT BE SUFFICIENT FOR TISAX LABELS!



TISAX

**PROCESO DE
CERTIFICACIÓN**

WELCOME TO ENX ASSOCIATION



TISAX

TISAX is an assessment and exchange mechanism for the information security of enterprises and allows recognition of assessment results among the participants. If you want... Read more

Sign in

Register



ENX NETWORK

ENX network is a joint solution from the European automotive industry for the secure exchange of critical development, purchasing, and production control data used by more than 1,000... Read more

Sign in

Register

SEGURIDAD DE LA INFORMACIÓN

1. POLÍTICAS Y ORGANIZACIÓN

- 1.1 Políticas de seguridad de la información (1)
- 1.2 Organización de la Seguridad de la Info (4)
- 1.3 Gestión de activos (3)
- 1.4 Gestión de riesgos de SI (1)
- 1.5 Evaluaciones (2)
- 1.6 Gestión de incidencias (1)

2. RECURSOS HUMANOS

- 2. Recursos Humanos (4)

3. SECUZA FÍSICA Y CONTINUIDAD DEL NEGOCIO

- 3. Seguridad física y continuidad del negocio (4)

4. GESTIÓN DE IDENTIDADES Y ACCESOS

- 4.1 Gestión de identidades (3)
- 4.2 Gestión de accesos (1)

5. SEGURIDAD INFORMÁTICA / CIBERSEGURIDAD

- 5.1 Criptografía (2)
- 5.2 Seguridad de la operación (7)
- 5.3 Adquisiciones del sistema, ges. req. Y des(4)

6. RELACIONES CON PROVEEDORES

- 6. Relaciones con proveedores (2)

7. CUMPLIMIENTO

- 7. Cumplimiento (2)

PROTECCIÓN DE PROTOTIPOS

8. PROTECCIÓN DE PROTOTIPOS

- 8.1 Seguridad física y ambiental (8)
- 8.2 Requisitos organizativos (7)
- 8.3 Manipulación de vehículos, com. y partes (2)
- 8.4 Requisitos para los vehículos de prueba (3)
- 8.5 Requisitos para eventos y pruebas (2)

PROTECCIÓN DE DATOS

9. PROTECCIÓN DE DATOS

- 9. Protección de datos (4)

SEGUIMIENTO

- ☐ El seguimiento es necesario para evaluación la eficacia de las acciones del PAC
 - ☐ Si no hay hallazgos, el informe y las Etiquetas TISAX se actualizarán
 - ☐ En caso contrario, el PAC tiene que ser actualizado
 - ☐ Las evaluaciones de seguimiento pueden ser una reunión física o en remoto
- El propósito de la "evaluación de seguimiento" es evaluar si se resuelven todas las no conformidades previamente identificadas (hallazgos menores o mayores).
- El participante suele solicitar la evaluación de seguimiento una vez que está seguro de que se han eliminado todas las no conformidades.
- Si durante una evaluación de seguimiento el auditor sigue detectando no conformidades existentes o incluso nuevas, el PAC debe ser actualizado y esta parte del proceso de evaluación comienza de nuevo.

SEGUIMIENTO

INTERCAMBIO INFORMACIÓN

6

PLAN ACCIONES

5

4

AUDITORÍA

3

PREPARACIÓN

2

NECESIDAD

1

TISAX

**PROCESO DE
CERTIFICACIÓN**

SEGUIMIENTO

- Puede haber tantas evaluaciones de seguimiento como sean necesarias.
- La evaluación de seguimiento puede ser remotamente o presencial.
- Después de una evaluación de seguimiento sin que existan no conformidades, la empresa obtiene las etiquetas TISAX para el período de tiempo 36 meses (desde el final de la fecha de evaluación inicial).
- El PAC y el seguimiento podrían repetirse varias veces antes de 9 meses desde la evaluación inicial.



SEGUIMIENTO

6

INTERCAMBIO INFORMACIÓN

PLAN ACCIONES

5

4

AUDITORÍA

3

PREPARACIÓN

2

NECESIDAD

1

TISAX
**PROCESO DE
CERTIFICACIÓN**

SEGUIMIENTO

INTERCAMBIO INFORMACIÓN

PLAN ACCIONES

AUDITORÍA

PREPARACIÓN

NECESIDAD

TISAX

PROCESO DE CERTIFICACIÓN



Avda. Los Olmos, 1
01013 Vitoria-Gasteiz (Álava)



+34 945 33 05 37



jm.moreno@sccconsulting.es



SCC Consulting



<https://www.linkedin.com/company/sccconsulting>



<https://facebook.com/sccconsulting>



<https://twitter.com/sccconsulting>