Manual del participante de TISAX

Lleve a cabo el proceso de evaluación TISAX y comparta el resultado de la evaluación con sus socios

Publicado por

ENX Association
asociación según la ley francesa de 1901,
con núm. de registro w923004198 en la Sous-préfecture de Boulogne-Billancourt, Francia

Direcciones
20 rue Barthélémy Danjou, 92100 Boulogne-Billancourt, Francia
Bockenheimer Landstraße 97-99, 60325 Fráncfort del Meno, Alemania

Autor

Florian Gleich

Contacto

tisax@enx.com
+49 69 9866927-77

Versión

Fecha:	2023-12-07
Versión:	2.7
Clasificación:	Public
ENX doc ID:	602-ES

Aviso de copyright

Todos los derechos reservados por ENX Association.
ENX, TISAX y los logotipos correspondientes son marcas registradas de ENX Association.
Las marcas comerciales de terceros que se mencionan pertenecen a sus respectivos propietarios.

Índice

1. Sinopsis . . . 8
1.1. Finalidad . . . 8
1.2. Alcance . . . 8
1.3. Destinatarios . . . 9
1.4. Estructura . . . 9
1.5. Cómo usar este documento . . . 9
1.6. Contacto . . . 10
1.7. El manual del participante de TISAX en otros idiomas y formatos . . . 10
1.7.1. Acerca de la traducción al español . . . 13
1.7.2. Acerca del formato online . . . 13
1.7.3. Acerca del formato offline . . . 13
1.7.4. Acerca del formato PDF . . . 14
2. Introducción . . . 15
2.1. ¿Por qué TISAX? . . . 15
2.2. ¿Quién define qué significa "seguro"? . . . 15
2.3. El camino de la automoción . . . 16
2.4. ¿Cómo demostrar la seguridad de forma eficiente? . . . 16
3. El proceso TISAX . . . 18
3.1. Sinopsis . . . 18
3.2. Registro . . . 19
3.3. Evaluación . . . 19
3.4. Intercambio . . . 20
4. Registro (paso 1) . . . 21
4.1. Sinopsis . . . 21
4.2. Usted es un participante de TISAX . . . 21
4.3. Preparación del registro . . . 24
4.3.1. La base legal . . . 24
4.3.2. El alcance de la evaluación TISAX . . . 25
4.3.2.1. Descripción del alcance . . . 26
4.3.2.2. Alcance estándar . . . 26
4.3.2.3. Determinación del alcance . . . 27
4.3.2.4. Personalización del alcance . . . 28
4.3.2.5. Ubicaciones dentro del alcance . . . 30
4.3.2.6. Nombre del alcance . . . 33
4.3.2.7. Contactos . . . 34

4.3.2.8. Publicación y divulgación . . . 35
4.3.3. Objetivos de evaluación . . . 37
4.3.3.1. Lista de objetivos de evaluación . . . 37
4.3.3.2. Objetivos de evaluación e ISA . . . 40
4.3.3.3. Objetivos de evaluación y etiquetas TISAX . . . 40
4.3.3.4. Selección de los objetivos de evaluación . . . 41
4.3.3.5. Necesidad de protección y niveles de evaluación . . . 45
4.3.3.6. Objetivos de evaluación y sus propios proveedores . . . 50
4.3.4. Tasa . . . 50
4.4. Portal ENX . . . 53
4.5. Proceso de registro online . . . 53
4.5.1. Tiempo necesario . . . 53
4.5.2. Empiece aquí . . . 53
4.5.3. Cuenta en el portal . . . 54
4.5.4. Registro como participante . . . 54
4.5.5. Contacto del participante . . . 54
4.5.6. Condiciones generales . . . 56
4.5.7. Registro del alcance de la evaluación . . . 56
4.5.8. Mensaje de correo electrónico de confirmación . . . 59
4.5.8.1. Participant ID (ID de participante) . . . 60
4.5.8.2. Scope ID (ID de alcance) . . . 61
4.5.9. Información de estado . . . 62
4.5.10. Cambios en su información de registro . . . 65
5. Evaluación (paso 2) . . . 66
5.1. Sinopsis . . . 66
5.2. Autoevaluación basada en la ISA . . . 66
5.2.1. Descarga del documento ISA . . . 67
5.2.2. Entender el documento ISA . . . 67
5.2.2.1. Catálogos de criterios . . . 67
5.2.2.2. Capítulos . . . 75
5.2.2.3. Preguntas de control . . . 75
5.2.2.4. Campos del formulario de autoevaluación . . . 76
5.2.2.5. Objetivo . . . 77
5.2.2.6. Requisitos . . . 78
5.2.2.7. Niveles de madurez . . . 78
5.2.3. Realizar la autoevaluación . . . 80
5.2.4. Interpretar el resultado de la autoevaluación . . . 81

5.2.4.1. Análisis . . . 81
5.2.4.2. El nivel de madurez objetivo (a nivel de pregunta) . . . 85
5.2.4.3. Su resultado (a nivel de pregunta) . . . 85
5.2.4.4. El objetivo (a nivel de puntuación) . . . 88
5.2.4.5. Su resultado (a nivel de puntuación) . . . 90
5.2.4.6. ¿Está listo? . . . 91
5.2.5. Examine el resultado de la autoevaluación . . . 93
5.3. Selección del proveedor de auditoría . . . 94
5.3.1. Información de contacto . . . 95
5.3.2. Cobertura . . . 95
5.3.3. Solicitud de ofertas . . . 95
5.3.4. Valoración de las ofertas . . . 96
5.4. Proceso de evaluación TISAX . . . 98
5.4.1. Sinopsis . . . 98
5.4.2. Reunión inicial . . . 98
5.4.3. Tipos de evaluación TISAX . . . 99
5.4.4. Elementos de la evaluación TISAX . . . 100
5.4.5. Acerca de la conformidad . . . 100
5.4.6. Su preparación para el proceso de evaluación TISAX . . . 103
5.4.7. Evaluación inicial . . . 103
5.4.7.1. La primera reunión inicial formal . . . 104
5.4.7.2. Procedimiento de evaluación . . . 104
5.4.7.3. Reunión final . . . 104
5.4.7.4. Informe de evaluación TISAX . . . 104
5.4.8. Preparación del plan de acciones correctivas . . . 105
5.4.9. Evaluación del plan de acciones correctivas . . . 106
5.4.9.1. Motivos de una evaluación del plan de acciones correctivas . . . 107
5.4.9.2. Combinación con la evaluación inicial . . . 107
5.4.9.3. Requisitos del plan de acciones correctivas . . . 107
5.4.9.4. Etiquetas TISAX temporales . . . 108
5.4.10. Evaluación de seguimiento . . . 109
5.4.10.1. Calendario . . . 109
5.4.10.2. Requisitos previos . . . 109
5.4.10.3. Vencimiento de las etiquetas TISAX temporales . . . 109
5.4.11. Diagrama del proceso de evaluación TISAX . . . 109
5.4.12. Assessment ID (ID de evaluación) . . . 113
5.4.13. Informe de evaluación TISAX . . . 114

5.4.14. Etiquetas TISAX . . . 115
5.4.14.1. Jerarquía de las etiquetas TISAX . . . 116
5.4.14.2. Periodo de validez de las etiquetas TISAX . . . 117
5.4.14.3. Renovación de las etiquetas TISAX . . . 117
6. Intercambio (paso 3) . . . 119
6.1. Premisa . . . 119
6.2. La plataforma de intercambio . . . 119
6.3. Requisitos previos generales . . . 119
6.4. Permanencia de los resultados intercambiados . . . 120
6.5. Niveles de divulgación . . . 120
6.6. Publicar el resultado de la evaluación en la plataforma de intercambio . . . 121
6.7. Compartir el resultado de la evaluación con un participante concreto . . . 122
6.7.1. Requisitos previos . . . 123
6.7.2. Cómo crear permisos de divulgación . . . 124
6.8. Compartir el resultado de la evaluación fuera de TISAX . . . 125
6.8.1. Las razones de este estricto mecanismo de intercambio . . . 125
6.8.2. Una guía para escribir en público sobre TISAX . . . 125
6.8.3. Cómo compartir el resultado con un socio que todavía no es participante de TISAX 126
6.8.4. Cómo compartir el resultado con empleados de su socio que no tienen acceso directo al portal ENX . . . 126
7. Anexos . . . 128
7.1. Anexo: Ejemplo de factura . . . 128
7.2. Anexo: Ejemplo de mensaje de correo electrónico de confirmación . . . 129
7.3. Anexo: Ejemplo de TISAX Scope Excerpt . . . 130
7.4. Anexo: Participant status (Estado del participante) . . . 131
7.4.1. Sinopsis: Participant status (Estado del participante) . . . 131
7.4.2. Participant status “Incomplete” (Estado del participante “Incompleto”) . . . 133
7.4.3. Participant status “Awaiting approval” (Estado del participante “Pendiente de aprobación”) . . . 134
7.4.4. Participant status “Preliminary” (Estado del participante “Preliminar”) . . . 134
7.4.5. Participant status “Registered” (Estado del participante “Registrado”) . . . 136
7.4.6. Participant status “Expired” (Estado del participante “Expirado”) . . . 137
7.5. Anexo: Assessment scope status (Estado del alcance de la evaluación) . . . 137
7.5.1. Sinopsis: Assessment scope status (Estado del alcance de la evaluación) . . . 137
7.5.2. Assessment scope status “Incomplete” (Estado del alcance de la evaluación “Incompleto”) . . . 139
7.5.3. Assessment scope status “Awaiting your order” (Estado del alcance de la

evaluación “Pendiente del pedido”) . . . 140
7.5.4. Assessment scope status “Awaiting ENX approval” (Estado del alcance de la evaluación “Pendiente de aprobación ENX”) . . . 140
7.5.5. Assessment scope status “Awaiting your payment” (Estado del alcance de la evaluación “Pendiente de pago”) . . . 141
7.5.6. Assessment scope status “Registered” (Estado del alcance de la evaluación “Registrado”) . . . 142
7.5.7. Assessment scope status “Active” (Estado del alcance de la evaluación “Activo”) 142
7.5.8. Assessment scope status “Expired” (Estado del alcance de la evaluación “Expirado”) . . . 142
7.6. Anexo: Assessment status (Estado de la evaluación) . . . 144
7.6.1. Sinopsis: Assessment status (Estado de la evaluación) . . . 144
7.6.2. Assessment status “Initial assessment ordered” (Estado de la evaluación “Evaluación inicial solicitada”) . . . 146
7.6.3. Assessment status “Initial assessment ongoing” (Estado de la evaluación “Evaluación inicial en curso”) . . . 146
7.6.4. Assessment status “Waiting for corrective action plan assessment” (Estado de la evaluación “A la espera de la evaluación del plan de acciones correctivas”) . . . 147
7.6.5. Assessment status “Waiting for follow-up” (Estado de la evaluación “A la espera del seguimiento”) . . . 147
7.6.6. Assessment status “Finished” (Estado de la evaluación “Finalizado”) . . . 148
7.7. Anexo: El razonamiento en contra de las “pre-evaluaciones” y los “análisis de deficiencias” . . . 148
7.8. Anexo: Alcances personalizados . . . 150
7.8.1. Alcance ampliado personalizado . . . 150
7.8.2. Alcance completamente personalizado . . . 150
7.9. Anexo: Gestión del ciclo de vida de los datos del participante . . . 151
7.9.1. Pérdida de acceso a los datos de participante (portal ENX) . . . 151
7.9.2. Administración de contactos . . . 151
7.9.2.1. Cómo añadir un nuevo contacto . . . 152
7.9.2.2. Cómo borrar un contacto existente . . . 152
7.9.2.3. Cómo actualizar los datos de un contacto existente . . . 153
7.9.3. Administración de ubicaciones . . . 153
7.9.3.1. Cómo solicitar el cambio de nombre de su empresa . . . 154
7.9.3.2. Cómo solicitar un cambio de ubicación . . . 154
7.9.3.3. Cómo solicitar el cambio de nombre de la calle . . . 155
7.9.3.4. Cómo añadir una ubicación adicional . . . 156

7.10. Anexo: Evaluación de la ampliación del alcance . . . 156
7.11. Anexo: Gestión del ciclo de vida ISA . . . 157
7.12. Anexo: Documentos útiles . . . 158
7.13. Anexo: Gestión de reclamaciones . . . 159
7.13.1. Motivos de reclamación . . . 159
7.13.1.1. Reclamaciones sobre ENX Association . . . 159
7.13.1.2. Reclamaciones sobre los proveedores de auditoría . . . 159
7.13.1.3. Requisitos de las reclamaciones . . . 159
7.13.2. Contacto para reclamaciones . . . 160
8. Historial del documento . . . 161

1. Sinopsis

1.1. Finalidad

Le damos la bienvenida a TISAX (Trusted Information Security Asessment Exchange o intercambio confiable de evaluación de seguridad de la información).

Uno de sus socios le ha solicitado que demuestre que su gestión de la seguridad de la información cumple un nivel definido de acuerdo con los requisitos de la “Evaluación de la seguridad de la información” (ISA, por sus siglas en inglés). De forma que quiere comprobar si cumple estos requisitos.

El objetivo de este manual es permitirle satisfacer la solicitud de su socio o bien anticiparse antes de que se lo soliciten.

El manual describe los pasos que debe seguir para superar la evaluación TISAX y para compartir el resultado de la evaluación con sus socios.

Establecer y mantener un sistema de gestión de la seguridad de la información (ISMS, por sus siglas en inglés) ya es una tarea compleja. Demostrar a sus socios que ese sistema de gestión de la seguridad de la información está a la altura añade aún más complejidad. Este manual no le ayudará a gestionar la seguridad de la información. Sin embargo, pretende hacer que la tarea de demostrar a sus socios su empeño sea lo más fácil posible.

1.2. Alcance

Este manual hace referencia a todos los procesos TISAX en los que pueda participar.

Contiene todo lo que necesita saber para llevar a cabo el proceso TISAX.

El manual ofrece asesoramiento sobre cómo tratar los requisitos en materia de seguridad de la

información en el marco de la evaluación. Sin embargo, no pretende informarle en general sobre lo que tiene que hacer para superar la evaluación de seguridad de la información.

1.3. Destinatarios

Los principales destinatarios de este manual son empresas que necesitan o quieren demostrar un nivel definido de gestión de la seguridad de la información de acuerdo con la “Evaluación de la seguridad de la información (ISA)”.

Tan pronto como se involucre activamente en los procesos TISAX, se beneficiará de la información que contiene este manual.

También se beneficiarán las empresas que solicitan a sus proveedores que demuestren niveles definidos de gestión de la seguridad de la información. Este manual les permite entender qué deben hacer sus proveedores para satisfacer esa demanda.

1.4. Estructura

Empezaremos con una breve introducción a TISAX y, a continuación, pasaremos a dar instrucciones sobre CÓMO hacer las cosas. Encontrará todo lo que necesita saber para llevar a cabo el proceso, en el orden en que necesita saberlo.

El tiempo de lectura estimado de este documento es de 75-90 minutos.

1.5. Cómo usar este documento

Tarde o temprano, querrá entender la mayor parte de las cosas descritas en este documento. Para prepararse adecuadamente, le recomendamos la lectura del manual completo.

Hemos estructurado el manual según los tres pasos principales del proceso TISAX, de forma que puede ir la sección que necesita y leer el resto más tarde.

El manual utiliza ilustraciones para facilitar la comprensión. Los colores de las ilustraciones a menudo tienen un significado adicional. Por tanto, le recomendamos que lea el documento en una pantalla o como impresión a color.

Agradecemos sus comentarios. Si cree que falta algo en este manual o que no se entiende fácilmente, no dude en hacérnoslo saber. Nosotros y los futuros lectores agradecerán los comentarios.

Si ya ha usado una versión anterior del manual del participante de TISAX, encontrará algunas notas importantes al final del documento en la Sección 8, “Historial del documento”.

1.6. Contacto

Estamos a su disposición para guiarle a lo largo del proceso TISAX y para responder cualquier duda que se le plantee.

Envíenos un mensaje de correo electrónico a:	tisax@enx.com
O llámenos al:	+49 69 9866927-77

Nos podrá localizar durante el horario de oficina habitual de Alemania (UTC+01:00).

Todos hablamos inglés y alemán. Uno de nuestros compañeros es hablante nativo de italiano.

Tenga en cuenta la Sección 7.13, “Anexo: Gestión de reclamaciones”.

1.7. El manual del participante de TISAX en otros idiomas y formatos

El manual del participante de TISAX está disponible en los siguientes idiomas y formatos:

Idioma	Versión	Formato	Enlace
Inglés	2.7	Online	https://www.enx.com/handbook/tisax-participant-handbook.html
		Offline	https://www.enx.com/handbook/tisax-participant-handbook-offline.html
		PDF	https://www.enx.com/handbook/TISAX%20Participant%20Handbook.pdf

Idioma	Versión	Formato	Enlace
Alemán	2.7	Online	https://www.enx.com/handbook/tisax-teilnehmerhandbuch.html
		Offline	https://www.enx.com/handbook/tisax-teilnehmerhandbuch-offline.html
		PDF	https://www.enx.com/handbook/TISAX-Teilnehmerhandbuch.pdf
Francés	2.7	Online	https://www.enx.com/handbook/tph-fr.html
		Offline	https://www.enx.com/handbook/tph-fr-offline.html
		PDF	https://www.enx.com/handbook/tph-fr.pdf
Chino	2.7	Online	https://www.enx.com/handbook/tph-cn.html
		Offline	https://www.enx.com/handbook/tph-cn-offline.html
		PDF	https://www.enx.com/handbook/tph-cn.pdf
Español	2.7	Online	https://www.enx.com/handbook/tph-es.html
		Offline	https://www.enx.com/handbook/tph-es-offline.html
		PDF	https://www.enx.com/handbook/tph-es.pdf
Japonés	2.7	Online	https://www.enx.com/handbook/tph-jp.html
		Offline	https://www.enx.com/handbook/tph-jp-offline.html
		PDF	https://www.enx.com/handbook/tph-jp.pdf
Portugués (Brasil)	2.7	Online	https://www.enx.com/handbook/tph-pt.html
		Offline	https://www.enx.com/handbook/tph-pt-offline.html
		PDF	https://www.enx.com/handbook/tph-pt.pdf
Italiano	2.7	Online	https://www.enx.com/handbook/tph-it.html
		Offline	https://www.enx.com/handbook/tph-it-offline.html
		PDF	https://www.enx.com/handbook/tph-it.pdf

Idioma	Versión	Formato	Enlace
Coreano	2.7	Online	https://www.enx.com/handbook/tph-kr.html
		Offline	https://www.enx.com/handbook/tph-kr-offline.html
		PDF	https://www.enx.com/handbook/tph-kr.pdf

Nota importante:

La versión en inglés es la versión principal.
El resto de versiones son traducciones del texto inglés.
En caso de duda, la versión en inglés prevalece.

1.7.1. Acerca de la traducción al español

Este Manual del participante de TISAX es una traducción del texto inglés.

Todos los documentos que se utilizan en TISAX se han creado en inglés (p. ej., todos los contratos y requisitos para los proveedores de servicios de auditoría TISAX). Como resultado, su socio o proveedor de auditoría puede usar algunos términos específicos de TISAX en inglés.

Para que pueda asignarlos correctamente, o bien hemos dejado el término original TISAX en inglés en la traducción del Manual del participante de TISAX, o bien hemos incluido el término en inglés entre paréntesis detrás de la traducción.

1.7.2. Acerca del formato online

Cada sección tiene un ID único (formato: ID1234).
El ID hace referencia a una sección específica, independientemente del idioma.

Si quiere desplazarse a una sección específica, puede:

- hacer clic con el botón derecho sobre el título de la sección y copiar el enlace, o bien
- hacer clic sobre el título de la sección y copiar el enlace de la barra de dirección de su navegador.

La mayoría de figuras están disponibles en un tamaño mayor al mostrado de forma predeterminada. Haga clic sobre la figura para abrir la versión mayor.

1.7.3. Acerca del formato offline

El formato offline mantiene la mayoría de funciones del formato online. En particular, las figuras están incrustadas en el archivo HTML. Solo necesita un archivo para usar el formato offline.

En comparación con el formato online, el formato offline no cuenta con lo siguiente:

- las imágenes de mayor tamaño
- las fuentes originales del formato online
  Los ajustes predeterminados de su navegador definirán las fuentes.

1.7.4. Acerca del formato PDF

Si usa el formato PDF en su PC, podrá hacer clic en todas las referencias. Pero, si imprime la versión en PDF, no tendrá remisiones a través de los números de página y deberá buscar las referencias por su cuenta.

2. Introducción

Las siguientes secciones presentan el concepto TISAX.

Si tiene prisa, puede saltárselas y empezar directamente en la Sección 4.3, “Preparación del registro”.

2.1. ¿Por qué TISAX?

O, más bien, ¿por qué está usted aquí?

Para contestar a estas preguntas, empezaremos con algunas reflexiones sobre los negocios en general y la protección de la información en particular.

Imagínese a su socio. Tiene información confidencial. Quiere compartir esa información con su proveedor, usted. La cooperación entre usted y su socio crea valor. La información que su socio comparte con usted es una parte importante de esa creación de valor. Por tanto, quiere protegerla de forma adecuada. Y quiere asegurarse de que usted trata su información con el mismo cuidado.

Pero ¿cómo puede saber que su información está en buenas manos? No puede simplemente “creerle”. Su socio debe tener alguna prueba.

Llegados a este punto, hay dos cuestiones. ¿Quién define qué es un manejo “seguro” de la información? Y, ¿cómo se demuestra?

2.2. ¿Quién define qué significa "seguro"?

Usted y su socio no son los únicos que se enfrentan a estas cuestiones por primera vez. Prácticamente todo el mundo tiene que encontrarles respuesta, y la mayoría de respuestas se parecerán.

En lugar de crear una solución independiente cada vez a un problema común, un método estándar le evita tener que partir de cero. Si bien definir un estándar supone un gran esfuerzo, solo se hace una vez y los que vienen detrás se benefician de ello cada vez.

Seguro que hay distintas opiniones sobre lo que hay que hacer para proteger la información. Pero, por las ventajas indicadas antes, la mayoría de las empresas apuestan por los estándares. Un estándar contiene de forma condensada todas las mejores prácticas, probadas en el tiempo y acreditadas, para hacer frente a un reto concreto.

En nuestro caso, los estándares como ISO/IEC 27001 (sobre los sistemas de gestión de la seguridad de la información, o ISMS) y su implementación establecen una forma reconocida de manejar de forma segura la información confidencial. Un estándar como este le evita tener que reinventar la rueda cada vez. Y, aún más importante, los estándares constituyen una base

común cuando dos empresas necesitan intercambiar datos confidenciales.

2.3. El camino de la automoción

Por naturaleza, los estándares independientes de la industria se diseñan como soluciones de talla única, y no a medida de las necesidades concretas de las empresas de automoción.

Hace cierto tiempo, el sector del automóvil formó asociaciones con el objetivo --entre otros-- de perfeccionar y definir estándares ajustados a sus necesidades específicas. La Asociación Alemana de la Industria Automotriz (VDA) es una de ellas. En el grupo de trabajo encargado de la seguridad de la información, diversos miembros del sector llegaron a la conclusión de que tienen necesidades similares suficientes como para ajustar a medida los estándares de gestión de la seguridad de la información.

Su esfuerzo conjunto se tradujo en un cuestionario que cubre los requisitos de seguridad de la información ampliamente aceptados por la industria del automóvil. Se llama la “Evaluación de la seguridad de la información” (ISA, por sus siglas en inglés).

Con la ISA, tenemos una respuesta a la pregunta “¿Quién define qué significa ‘seguro’?” A través de la VDA, la industria automotriz ofrece esta respuesta a sus miembros.

2.4. ¿Cómo demostrar la seguridad de forma eficiente?

Mientras que algunas empresas usan la ISA únicamente con fines internos, otras la usan para evaluar la madurez de la gestión de la seguridad de la información de sus proveedores. En algunos casos, una autoevaluación es suficiente para la relación comercial. Sin embargo, en ciertos casos, las empresas llevan a cabo una evaluación completa de la gestión de la seguridad de la información de su proveedor (incluidas auditorías in situ).

Junto con la creciente conciencia de la necesidad de una gestión de la seguridad de la información y el aumento en la adopción de la ISA como herramienta para las evaluaciones de la seguridad de la información, cada vez más proveedores se enfrentaban a solicitudes similares de distintos socios.

Esos socios seguían aplicando estándares diferentes y tenían opiniones variadas sobre cómo interpretarlos. Sin embargo, los proveedores tenían que demostrar las mismas cosas, solo que de formas diferentes.

Y cuantos más proveedores debían probar a sus socios su nivel de gestión de la seguridad de la información, más fuertes se volvieron las quejas por tener que repetir el mismo esfuerzo una y otra vez. Mostrar a un auditor tras otro las mismas medidas de gestión de la seguridad de la información simplemente no es eficiente.

¿Qué se puede hacer para que esto sea más eficiente? ¿No ayudaría si el informe de un auditor

pudiera reutilizarse para distintos socios?

Los OEM y los proveedores que integran el grupo de trabajo de la ENX responsable de mantener la ISA escucharon las quejas de los proveedores. Ahora ofrecen una respuesta a sus proveedores, así como al resto de empresas del sector del automóvil, para la pregunta “¿Cómo demostrar la seguridad?”

La respuesta es TISAX, la abreviatura de “Trusted Information Security Assessment Exchange” (“intercambio confiable de evaluación de seguridad de la información”).

3. El proceso TISAX

3.1. Sinopsis

El proceso TISAX habitualmente[1] empieza con que uno de sus socios le solicita que pruebe un nivel definido de gestión de la seguridad de la información de acuerdo con los requisitos de la “Evaluación de la seguridad de la información” (ISA). Para responder a esta solicitud, debe completar el proceso TISAX de 3 pasos. Esta sección le proporciona un resumen de los pasos que deberá dar.

El proceso TISAX de 3 pasos consiste en:

Figura 1. Sinopsis del proceso TISAX

1. Paso 1
   Registro
2. Paso 2
   Evaluación
3. Paso 3
   Intercambio

1. Registro
   Recopilamos la información sobre su empresa y lo que debe formar parte de la evaluación.
2. Evaluación
   Usted lleva a cabo la evaluación o las evaluaciones, a cargo de uno de nuestros proveedores de auditoría TISAX.
3. Intercambio
   Comparte el resultado de la evaluación con sus socios.

Cada paso contiene subpasos. Estos se presentan en las tres secciones siguientes y se describen detalladamente en sus secciones correspondientes.

Recuerde:

Aunque nos gustaría poder decirle cuánto tiempo necesitará para obtener su resultado de evaluación TISAX, entienda que es algo que no podemos predecir de forma fiable. La duración total del proceso TISAX depende de demasiados factores. La gran variedad de tamaños de empresa y objetivos de evaluación, así como el respectivo grado de preparación del sistema de gestión de la

> seguridad de la información, hacen que sea imposible.

3.2. Registro

El primer paso es el registro TISAX.

El principal objetivo del registro TISAX es recopilar información sobre su empresa. Usamos un proceso de registro online para ayudarle a proporcionar esa información.

Es el requisito previo a todos los pasos siguientes. Está sujeto a una tasa.

Durante el proceso de registro online:

- Le solicitamos información de contacto y de facturación.
- Debe aceptar nuestras condiciones.
- Puede definir el alcance de su evaluación de la seguridad de la información.

Para empezar directamente con este paso, consulte la Sección 4, “Registro (paso 1)”.

El proceso de registro online se describe en detalle en la Sección 4.5, “Proceso de registro online”. No obstante, si quiere empezar ahora mismo, vaya a enx.com/en-US/TISAX/.

3.3. Evaluación

El segundo paso es llevar a cabo la evaluación de la seguridad de la información.

Existen cuatro subpasos:

a. Preparación de la evaluación
   Ha de preparar la evaluación. El grado de preparación dependerá del nivel de madurez actual de su sistema de gestión de la seguridad de la información. La preparación se debe basar en el catálogo ISA.
b. Selección del proveedor de auditoría
   Debe elegir uno de nuestros proveedores de auditoría TISAX.
c. Evaluación de la seguridad de la información
   Su proveedor de auditoría llevará a cabo la evaluación de acuerdo con el alcance necesario para cumplir los requisitos de su socio. Este proceso de evaluación constará de una auditoría inicial como mínimo.
   Si su empresa no supera la evaluación a la primera, el proceso de evaluación puede requerir pasos adicionales.
d. Resultado de la evaluación
   Una vez que su empresa haya superado la evaluación, el proveedor de auditoría le facilitará el informe de evaluación TISAX oficial. El resultado de su evaluación también recibirá

“etiquetas TISAX”[2].

Para más información sobre este paso, consulte la Sección 5, “Evaluación (paso 2)”.

3.4. Intercambio

El tercer y último paso es compartir el resultado de la evaluación con su socio. El contenido del informe de evaluación TISAX está estructurado en niveles. Puede decidir hasta qué nivel tendrá acceso su socio.

El resultado de la evaluación es válido durante tres años. Suponiendo que siga siendo proveedor del socio para entonces, tendrá que llevar a cabo el proceso de tres pasos de nuevo[3].

Para más información sobre este paso, consulte la Sección 6, “Intercambio (paso 3)”.

Ahora que ya tiene una idea básica del proceso TISAX, en las siguientes secciones encontrará información sobre cómo realizar cada paso.

4. Registro (paso 1)

El tiempo de lectura estimado de la sección de registro es de 30-40 minutos.

4.1. Sinopsis

El registro TISAX es el primer paso. Es el requisito previo a todos los pasos siguientes.

Las siguientes secciones le guiarán a través del registro:

1. Empezaremos explicando un nuevo término fundamental.
2. Después, le recomendaremos qué debería hacer para preparar el proceso de registro online.
3. A continuación, le guiaremos a través del proceso de registro online.

4.2. Usted es un participante de TISAX

En primer lugar, permítanos presentarle un nuevo término que es imprescindible entender. Hasta ahora, usted era el “proveedor”. Ahora está aquí para cumplir el requisito de su “cliente”. Sin embargo, TISAX no distingue entre estos dos roles. Para TISAX, cualquiera que se registre es un “participante”. Usted --al igual que su socio-- “participa” en el intercambio de los resultados de la evaluación de la seguridad de la información.

Figura 2. Registro para convertirse en participante de TISAX

1. Su empresa
2. Registro TISAX
3. Participante de TISAX

Para diferenciar los dos roles desde el principio, nos referimos a usted, el proveedor, como “participante activo”. Nos referimos a su socio como “participante pasivo”. Como “participante activo”, usted se somete a una evaluación TISAX y comparte el resultado de la evaluación con otros participantes. El “participante pasivo” es quien ha solicitado que se someta a la evaluación TISAX. El “participante pasivo” recibe el resultado de la evaluación.

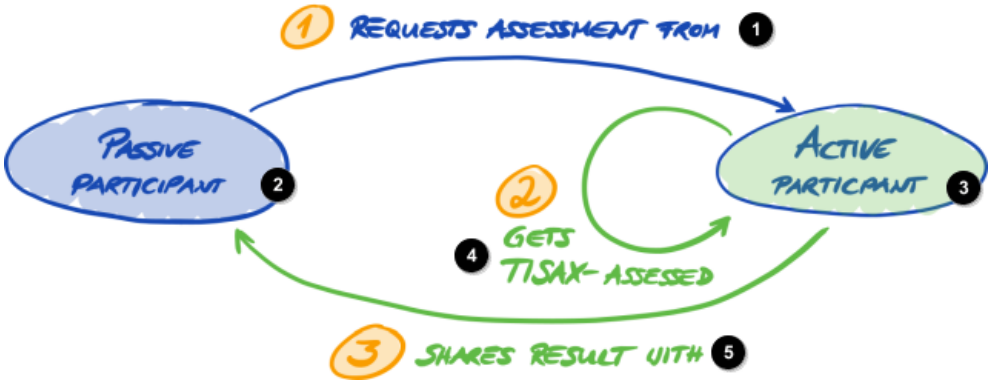


Figura 3. Participante pasivo y participante activo

1. 1 Solicita una evaluación del
2. Participante pasivo
3. Participante activo
4. 2 Se somete a una evaluación TISAX
5. 3 Comparte los resultados con el

Cualquier empresa puede tener los dos roles. Puede compartir el resultado de su evaluación con su socio, a la vez que solicita a sus propios proveedores que se sometan a la evaluación TISAX.

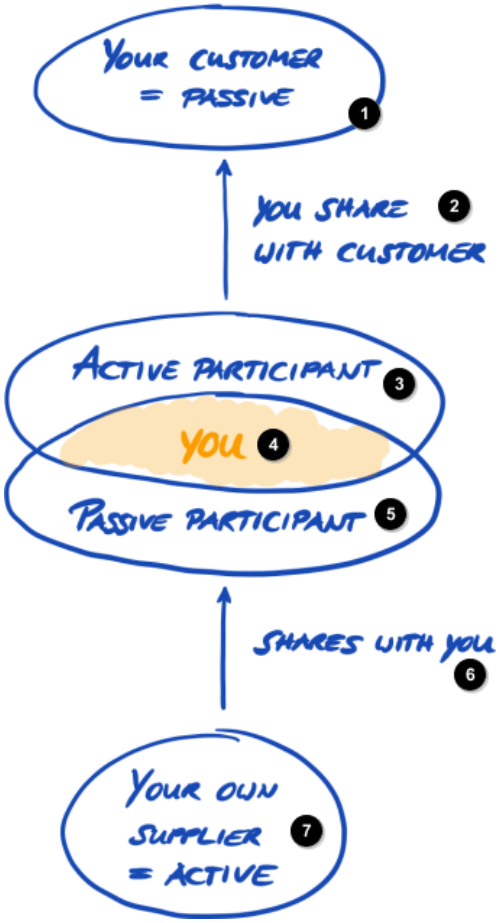


Figura 4. Los participantes de TISAX pueden ser activos y pasivos al mismo tiempo

1. Su cliente
   = pasivo
2. Usted comparte con el cliente
3. Participante activo
4. Usted
5. Participante pasivo
6. Comparte con usted
7. Su propio proveedor
   = activo

Solicitar a sus propios proveedores que se sometan a una evaluación TISAX puede ser especialmente recomendable si estos también manejan la información con necesidad de protección de su socio.

4.3. Preparación del registro

En esta sección le damos consejos sobre cómo *prepararse* para el registro. Describimos el proceso de registro en detalle en la Sección 4.5, “Proceso de registro online”.

Antes de iniciar el proceso de registro online, le recomendamos encarecidamente:

- que recopile la información por adelantado
- y que tome algunas decisiones.

4.3.1. La base legal

Normalmente, tendrá que firmar dos contratos. El primer contrato que suscribe es entre usted y ENX Association: las “Condiciones generales de participación en TISAX” (TISAX Participant GTCs). El segundo contrato es entre usted y uno de nuestros proveedores de auditoría TISAX. Para el registro, solo nos centraremos en el primer contrato.

Las Condiciones generales de participación en TISAX rigen nuestra relación mutua y su relación con otros participantes de TISAX. Definen los derechos y las obligaciones de todos nosotros. Además de las cláusulas habituales que encontrará en la mayoría de contratos, definen con detalle el manejo de la información intercambiada y obtenida durante el proceso TISAX. Un objetivo clave de estas reglas es mantener confidenciales los resultados de la evaluación TISAX. Como todos los participantes de TISAX están sujetos a las mismas normas, puede esperar una protección adecuada del resultado de su evaluación TISAX por parte de su socio (en su rol de participante pasivo).

Relativamente pronto en el proceso de registro online, le pediremos que acepte las Condiciones generales de participación en TISAX. Como se trata de un contrato real, le recomendamos que lea las Condiciones generales de participación en TISAX al iniciar el proceso de registro online. Uno de los motivos es que, en función del cargo que ocupe en su empresa, necesitará obtener una autorización de un abogado interno o externo.

Puede descargar las “Condiciones generales de participación en TISAX”[4] en nuestro sitio web en:
enx.com/en-US/TISAX/downloads/

Descarga directa en PDF:
enx.com/tisaxgtcen.pdf

Durante el proceso de registro online, le pediremos que marque dos casillas de verificación obligatorias:

- ☐ We accept the TISAX Participation General Terms and Conditions (Aceptamos las Condiciones generales de participación en TISAX)
- ☐ We confirm knowledge of Applicant’s release of Audit Providers’ professional duties of

secrecy acc. to Sec. IX.5. and X.3 of the TISAX Participation General Terms and Conditions; (Confirmamos conocer la exención del proveedor de auditoría de su obligación de confidencialidad según la sección IX.5. y X.3 de las Condiciones generales de participación en TISAX;)

Tenemos la segunda casilla de verificación porque algunos de nuestros proveedores de auditoría TISAX son auditores de cuentas. Los auditores de cuentas tienen requisitos especiales acerca del secreto profesional. Normalmente, los requisitos especiales acerca del secreto profesional prohíben a los auditores de cuentas de entre nuestros proveedores de auditoría compartir información con nosotros. En particular, esto anularía las opciones de control que necesitamos para desempeñar nuestra función de gobernanza. Por ese motivo necesitamos esa exención. Preste especial atención a dichas cláusulas antes de marcar la casilla de verificación.

Si suele exigir un acuerdo de confidencialidad (NDA, por sus siglas en inglés) entre usted y cualquiera que trate información confidencial, lea las secciones correspondientes de nuestras Condiciones generales. Deberían dar respuesta a todas sus inquietudes. Además, normalmente no tiene que facilitarnos ningún tipo de información confidencial.

Para finalizar la sección legal, entienda que el sistema depende de que todos acepten las mismas normas. Por tanto, no podemos aceptar condiciones generales adicionales[5].

4.3.2. El alcance de la evaluación TISAX

En el segundo paso del proceso TISAX, uno de nuestros proveedores de auditoría TISAX llevará a cabo la evaluación de la seguridad de la información. Para ello necesita saber dónde empezar y dónde acabar. Por tanto, debe definir un “alcance de la evaluación”.

El “alcance de la evaluación” describe el alcance que tendrá la evaluación de la seguridad de la información. Dicho de otra forma, cada parte de su empresa que maneje la información confidencial de su socio es parte del alcance de la evaluación. Puede considerarlo un elemento principal de la descripción de la tarea del proveedor de auditoría. Determina qué debe evaluar el proveedor de auditoría.

El alcance de la evaluación es importante por dos motivos:

a. El resultado de la evaluación solo satisfará los requisitos de su socio si su alcance cubre todas las partes de su empresa que manejan información del socio.
b. Un alcance de la evaluación definido con precisión es un requisito previo fundamental para el cálculo del coste por los proveedores de auditoría TISAX.

Nota importante:

ISO/IEC 27001 frente a TISAX

En primer lugar, debemos diferenciar dos tipos de alcance:

1) el alcance de su sistema de gestión de la seguridad de la información (ISMS) y
2) el alcance de la evaluación.
No tienen por qué ser idénticos.

Para la certificación ISO/IEC 27001, usted define el alcance de su ISMS (en la “declaración del alcance”). Tiene total libertad para definir el alcance de su ISMS. Sin embargo, el alcance de la evaluación (también conocido como “alcance de la auditoría”) debe ser idéntico al alcance del ISMS.

Para TISAX, también tiene que definir su ISMS. Pero el alcance de la evaluación puede ser diferente.

Para la certificación ISO/IEC 27001, puede configurar libremente el alcance de la evaluación definiendo el alcance de su ISMS.

Por contra, en el caso de TISAX, el alcance de la evaluación está predefinido. El alcance de la evaluación puede ser menor que el alcance de su ISMS. Pero debe encontrarse dentro del alcance de su ISMS.

4.3.2.1. Descripción del alcance

La descripción del alcance define el alcance de la evaluación. Para la descripción del alcance, ha de elegir uno de los dos tipos de alcance:

1. Standard scope (Alcance estándar)
2. Custom scope (Alcance personalizado)
    a. Custom extended scope (Alcance ampliado personalizado)
    b. Full custom scope (Alcance completamente personalizado)

En la siguiente sección trataremos el alcance estándar. El alcance estándar es la elección adecuada para más del 99 % de los participantes. Por eso, solo tratamos los alcances personalizados en la Sección 7.8, “Anexo: Alcances personalizados”.

4.3.2.2. Alcance estándar

La descripción de alcance estándar es la base para la evaluación TISAX. Otros participantes de TISAX solo aceptarán resultados de la evaluación basados en la descripción del alcance estándar.

La descripción del alcance estándar está predefinida y no puede cambiarla.

Una gran ventaja de contar con un alcance estándar es que usted no necesita pensar en su propia definición.

Esta es la descripción del alcance estándar (versión 2.0):

The TISAX assessment scope defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations.
The assessment is conducted at least in the highest assessment level listed in any of the listed assessment objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.

El alcance de la evaluación TISAX define el alcance que tiene la evaluación. La evaluación incluye todos los procesos, procedimientos y recursos bajo la responsabilidad de la organización evaluada que son relevantes para la seguridad de los objetos de protección y sus objetivos de protección, tal y como se definen en los objetivos de evaluación enumerados en las ubicaciones enumeradas.
La evaluación se lleva a cabo como mínimo en el nivel de evaluación más alto de cualquiera de los objetivos de evaluación enumerados. Todos los criterios de evaluación enumerados en los objetivos de evaluación se someten a evaluación.

Le recomendamos encarecidamente que elija el alcance estándar. Todos los participantes de TISAX aceptan los resultados de la evaluación de la seguridad de la información basados en el alcance estándar.

4.3.2.3. Determinación del alcance

Su próxima tarea después de definir el alcance es decidir qué ubicaciones forman parte del alcance de la evaluación.

Si su empresa es pequeña (una ubicación), es una tarea fácil. Simplemente ha de añadir su ubicación al alcance de la evaluación.

Si su empresa es grande, puede considerar la posibilidad de registrar más de un alcance de la evaluación.

Tener un único alcance que contenga todas las ubicaciones tiene ventajas:

- Tendrá un informe de evaluación, un resultado de la evaluación, una fecha de vencimiento.
- Podrá beneficiarse de costes reducidos para la evaluación porque el proveedor de auditoría TISAX solo ha de evaluar sus procesos, procedimientos y recursos centrales una sola vez.

Sin embargo, un único alcance también puede conllevar desventajas como:

- Todas las ubicaciones deben tener los mismos objetivos de evaluación.
- El resultado de su evaluación solo estará disponible cuando el proveedor de auditoría TISAX haya evaluado todas las ubicaciones. Este hecho puede ser importante si necesita el resultado de la evaluación con urgencia.
- El resultado de la evaluación dependerá de que todas las ubicaciones superen la evaluación. Si una sola ubicación no la supera, no obtendrá un resultado positivo de la evaluación. Para solventar esta situación puede: a) eliminar la ubicación del alcance, b) resolver los problemas, c) añadir la ubicación más tarde con una evaluación de ampliación del alcance.

4.3.2.4. Personalización del alcance

Solo usted puede dar respuesta a la pregunta de si le conviene tener un solo alcance o varios. Pero las preguntas del siguiente diagrama podrían ayudarle a decidir.

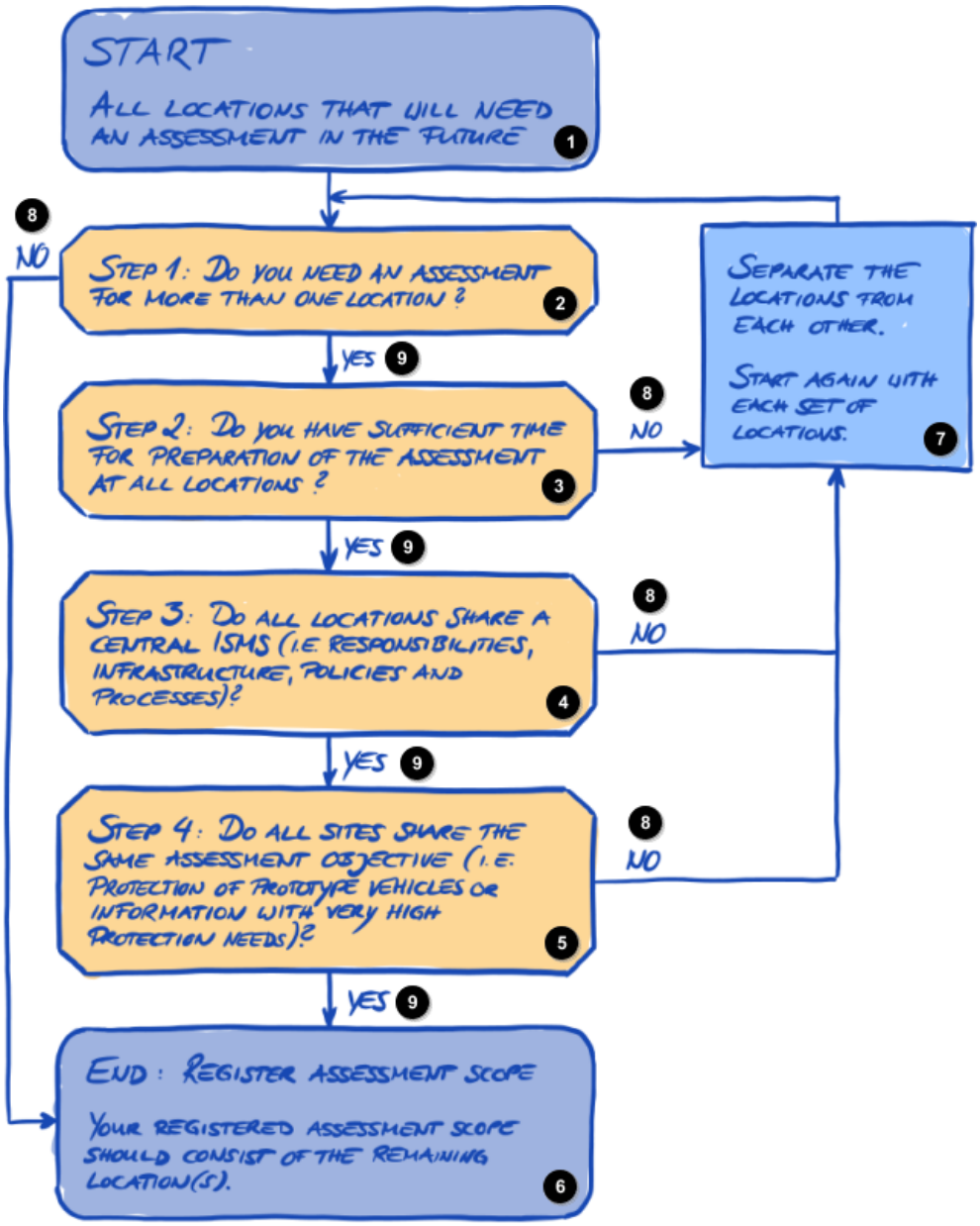


Figura 5. Diagrama de flujo de personalización del alcance

1. INICIO
   Todas las ubicaciones que necesitarán una evaluación en el futuro
2. Paso 1: ¿Necesita una evaluación para más de una ubicación?
3. Paso 2: ¿Tiene tiempo suficiente para preparar la evaluación de todas las ubicaciones?
4. Paso 3: ¿Todas las ubicaciones comparten un ISMS central (p. ej., responsabilidades, infraestructura, políticas y procesos)?
5. Paso 4: ¿Todas las sedes comparten el mismo objetivo de evaluación (p. ej., protección de vehículos prototipo o información con necesidad de protección muy alta)?

6. Fin: Registre el alcance de la evaluación
   El alcance de la evaluación registrado deberá incluir las ubicaciones restantes.
7. Separe las ubicaciones.
   Vuelva a empezar para cada conjunto de ubicaciones.
8. No
9. Sí

Recuerde:

No se deje intimidar por esta decisión. Puede cambiar cualquier alcance mientras el proveedor de auditoría no haya finalizado la evaluación.

Por ejemplo, durante la preparación de la evaluación podría darse cuenta de que el alcance no se ajusta y cambiarlo en consecuencia. O su proveedor de auditoría podría recomendarle que cambie el alcance durante las primeras fases de la evaluación.

Notas adicionales:

- Técnicamente, no puede cambiar el alcance de la evaluación que definió durante el proceso de registro online en el portal ENX. Pero el proveedor de auditoría puede actualizar el alcance de su evaluación cuando cargue el resultado de la misma en el portal ENX.
- Ampliar el alcance incrementa la tasa pero, si elimina alguna ubicación del alcance, no recibirá un reembolso. Dado que los proveedores de auditoría utilizan el alcance original como base para su cálculo de costes, también deberá esperar cambios.

4.3.2.5. Ubicaciones dentro del alcance

Una vez que haya decidido qué ubicaciones son parte del alcance de la evaluación, puede seguir recopilando información específica de cada ubicación.

Para cada ubicación solicitamos información como el nombre de la empresa y la dirección. También solicitamos información adicional que permita a nuestros proveedores de auditoría TISAX hacerse una mejor idea de la estructura de su empresa. Las respuestas serán la base para sus cálculos.

Prepárese para dar los siguientes datos de cada una de sus ubicaciones (el asterisco rojo * indica información obligatoria en el proceso online):

Campo	Opciones
Nombre de la ubicación *	n/a
Número D-U-N-S de D&B	n/a
Tipo de ubicación *	Edificio(s) en propiedad y de uso exclusivo de la empresa Edificio(s) alquilado(s) por la empresa Planta/oficina alquilada por la empresa en un edificio compartido Oficina compartida con otras empresas Centro de datos propio Centro de datos compartido
Protección pasiva de la ubicación *	Sí No
Industria *(Se permite la selección múltiple)*	Tecnología de la información ☐ Servicios informáticos ☐ Servicios de telecomunicación ☐ Desarrollo de software
	Gestión ☐ Consultoría
	Medios de comunicación ☐ Marketing ☐ Agencia ☐ Servicios de impresión ☐ Fotografía ☐ Servicios de traducción
	Investigación y desarrollo ☐ Inspección de vehículos ☐ Simulación de vehículos ☐ Construcción de prototipos ☐ Modelos de coches en miniatura ☐ Servicios de desarrollo ☐ Servicios de desarrollo CAx

Campo	Opciones
	Producción • Servicios de producción • Fabricación por encargo • Taller • Logística
	Ventas y servicios posventa • Importación, NSC • Concesionario • Servicios financieros • Seguros • Liquidación de siniestros
	Otra industria *(indique cuál)*
Empleados en la ubicación: en total *	0 1-10 11-100 101-1000 1001-5000 Más de 5000
Empleados en la ubicación: TI *	0 1-10 11-25 26-50 Más de 50
Empleados en la ubicación: seguridad informática *	0 A tiempo parcial 1-5 6-25 Más de 25
Empleados en la ubicación: seguridad de la ubicación *	0 A tiempo parcial 1-3 4-10 Más de 10

Campo	Opciones
Certificaciones de esta ubicación	ISO 27001 Otra *(indique cuál)* ISAE 3402 SOC2

Tabla 1. Información específica de la ubicación

Recuerde:

En el apartado “Industria”: seleccione una a su mejor saber y entender. No hay respuestas correctas y equivocadas al seleccionar las opciones. Si no encuentra una opción que se ajuste a su tipo de negocio, introduzca la opción adecuada en “Otra”.

Para cada ubicación deberá especificar un “location name” (“nombre de la ubicación”). El objetivo del nombre de la ubicación es que resulte más fácil referirse a la ubicación a la hora de asignarle un alcance de la evaluación.

Recomendamos que asigne nombres de ubicación siguiendo este esquema:

Esquema: [Referencia geográfica]

Ejemplo: para la empresa ficticia “ACME”

- Fráncfort
  (para una ubicación en la **ciudad** alemana de Fráncfort)

4.3.2.6. Nombre del alcance

Para cada alcance ha de especificar un “scope name” (“nombre del alcance”). La finalidad principal del nombre del alcance es facilitarle la identificación del alcance en la lista general de alcances del portal ENX. Le recomendamos que asigne un nombre que sea útil para el lector y sus compañeros. Para la comunicación externa, deberá utilizar el ID de alcance.

Puede especificar el nombre que quiera. Pero no dé el mismo nombre de alcance a más de un alcance.

Cuando más adelante quiera renovar su evaluación TISAX, necesitará crear un nuevo alcance (posiblemente, idéntico al actual). Por eso le recomendamos que añada el año de la evaluación al nombre del alcance.

Recomendamos asignar nombres de alcance siguiendo este esquema:

Esquema: [Referencia geográfica o *funcional*] [Año de la evaluación]

Ejemplos: para la empresa ficticia “ACME”

- 2024
  (sin referencia geográfica si su empresa solo tiene una ubicación)
- Fráncfort 2024
  (para un alcance con varias ubicaciones en la **localidad** alemana de Fráncfort)
- Baja Sajonia 2024
  (para un alcance con varias ubicaciones en el **estado** alemán de Baja Sajonia)
- Alemania 2024
  (para un alcance con varias ubicaciones en el **país** Alemania)
- EMEA 2024
  (para un alcance con todas las ubicaciones en la **región** EMEA (“Europa, Oriente Medio, África”))
- Desarrollo de prototipos 2024
  (referencia *funcional* para un alcance con todas las ubicaciones implicadas en el desarrollo de prototipos)

4.3.2.7. Contactos

Para poder comunicarnos con usted, recopilamos información de los contactos de su empresa.

Le pedimos como mínimo un contacto de su empresa como participante de TISAX en general y uno para cada alcance de evaluación. También puede proporcionar contactos adicionales.

Durante los preparativos para el registro, deberá decidir qué persona o personas de su empresa serán los contactos.

Pedimos los siguientes datos de contacto:

	Dato de contacto	¿Obligatorio?	Ejemplo
1.	Tratamiento	Sí	Sra., Sr.
2.	Grado académico		Dr., Ph.D., otros
3.	Nombre	Sí	John
4.	Apellido(s)	Sí	Doe
5.	Cargo	Sí	Responsable de TI
6.	Departamento	Sí	Tecnología de la información

	Dato de contacto	¿Obligatorio?	Ejemplo
7.	Número de teléfono principal	Sí	+49 69 986692777
8.	Número de teléfono secundario		
9.	Dirección de correo electrónico	Sí	john.doe@acme.com
10.	Idioma de preferencia	Sí	Inglés (predeterminado)
11.	Otros idiomas		Alemán, español
12.	Identificador personal		HPC 1234
13.	Dirección postal	Sí	Bockenheimer Landstraße 97-99
14.	Código postal	Sí	60325
15.	Localidad	Sí	Fráncfort
16.	Estado/provincia		
17.	País	Sí	Alemania

Tabla 2. Datos de contacto

Nota importante:

Recomendamos asignar al menos un sustituto para cada contacto. Si un contacto no está disponible temporalmente o abandona la empresa, otra persona podrá gestionar los datos de participante de su empresa.
Si necesita asignar un nuevo contacto (sin tener ningún otro contacto válido), deberá seguir un proceso complejo. Nuestro proceso asegura que solo las personas que pueden demostrar que están autorizadas a representar legalmente a la empresa puedan aprobar la asignación de un nuevo contacto principal.

4.3.2.8. Publicación y divulgación

El principal objetivo de TISAX es publicar el resultado de la evaluación para otros participantes de TISAX y compartir el resultado con su(s) socio(s).

Puede decidir la forma de publicar y compartir el resultado de la evaluación durante el proceso de registro o en cualquier momento posterior.

Si lleva a cabo el proceso TISAX como medida preventiva, puede decidir ya si publicar el resultado de la evaluación para la comunidad de participantes de TISAX. Si no es así, no hay nada que preparar en esta fase.

Si su socio le ha solicitado que lleve a cabo el proceso TISAX, tarde o temprano deberá compartir el resultado de la evaluación. Puede compartir ya la información de estado con su socio durante

el registro. En cuanto el resultado de la evaluación esté disponible, su socio tendrá permiso automáticamente para acceder al mismo[6].

Para compartir la información de estado, necesita dos cosas:

1. El ID de participante de TISAX de su socio

   El ID de participante de TISAX identifica a su socio como participante de TISAX.

   Normalmente, su socio debería proporcionarle su ID de participante de TISAX.

   Para mayor comodidad, nuestro formulario de registro incluye una lista desplegable con los ID de participante de algunas empresas que suelen recibir resultados de evaluación.[7]

2. El nivel de divulgación requerido

   El nivel de divulgación define hasta qué punto su socio puede acceder al resultado de la evaluación.

   Puede que su socio exija un nivel de divulgación específico o que usted decida hasta qué nivel quiere proporcionar acceso al resultado de su evaluación.

   Para más información sobre los niveles de divulgación, consulte la Sección 6.5, “Niveles de divulgación”.

Asegúrese de tener esta información.

Recuerde:

- Siempre puede optar por publicar el resultado de la evaluación más tarde.
- Siempre puede crear un permiso para su socio más tarde.

Nota importante:

Si no publica el resultado de la evaluación ni lo comparte, nadie podrá ver el resultado de la evaluación.

Nota importante:

No puede revocar la publicación o divulgación.

Para más información, consulte la Sección 6.4, “Permanencia de los resultados intercambiados”.

Recuerde:

> Puede sonar extraño, pero de hecho puede compartir su “resultado de evaluación” incluso sin haber iniciado el proceso de evaluación todavía. En esta fase inicial, solo está compartiendo el “estado de la evaluación”. El participante con el que comparta su “resultado de evaluación” verá en qué punto del proceso de evaluación se encuentra.
>
> Algunos participantes de TISAX tienen que emitir un comunicado especial si usted tiene que mostrar etiquetas de TISAX, pero aún no ha terminado el proceso de evaluación. En ese caso, es posible que su socio necesite ver su “estado de la evaluación” en su cuenta del portal ENX.
>
> Para más información sobre el estado de la evaluación, consulte la Sección 7.6, “Anexo: Assessment status (Estado de la evaluación)”.

Para más información sobre cómo publicar y compartir el resultado de su evaluación, consulte la Sección 6, “Intercambio (paso 3)”.

4.3.3. Objetivos de evaluación

Tiene que definir el o los objetivos de la evaluación durante el proceso de registro. El objetivo de la evaluación (assessment objective) determina los requisitos aplicables que debe cumplir su sistema de gestión de la seguridad de la información (ISMS). El objetivo de la evaluación se basa enteramente en el tipo de datos que trata por cuenta de su socio.

En las siguientes secciones, describimos los objetivos de evaluación y le aconsejamos para que pueda elegir el o los objetivos de evaluación correctos.

El uso de objetivos de evaluación facilita la comunicación con su socio y sus proveedores de auditoría TISAX porque hacen referencia a una entrada definida del proceso de evaluación TISAX.

> Recuerde:
>
> Algunos socios le pedirán la evaluación TISAX con un “nivel de evaluación” (AL, por sus siglas en inglés) determinado, en lugar de especificar el objetivo de evaluación.
>
> Para más información sobre los niveles de evaluación, consulte la Sección 4.3.3.5, “Necesidad de protección y niveles de evaluación” (subsección “Información adicional”).

4.3.3.1. Lista de objetivos de evaluación

Actualmente existen doce objetivos de evaluación TISAX. Debe seleccionar al menos un objetivo de evaluación. También puede seleccionar más de uno.

Considere el objetivo de evaluación como el punto de referencia para su sistema de gestión de la seguridad de la información. El objetivo de evaluación es una entrada clave del proceso TISAX. Todos los proveedores de auditoría TISAX basan su estrategia de evaluación en el objetivo de evaluación.

Los objetivos de evaluación TISAX actuales son:

Núm.	Nombre	Descripción
1.	Info high	Handling of information with high protection needs Manejo de información con necesidad de protección alta
2.	Info very high	Handling of information with very high protection needs Manejo de información con necesidad de protección muy alta
3.	Confidential	Handling of information with high protection needs in the context of confidentiality (access to confidential information) Manejo de información con necesidad de protección alta en el contexto de la confidencialidad (acceso a información confidencial)
4.	Strictly confidential	Handling of information with very high protection needs in the context of confidentiality (access to strictly confidential information) Manejo de información con necesidad de protección muy alta en el contexto de la confidencialidad (acceso a información estrictamente confidencial)
5.	High availability	Handling of information with high protection needs in the context of *availability* (high availability of information) Manejo de información con necesidad de protección alta en el contexto de la *disponibilidad* (disponibilidad alta de la información)
6.	Very high availability	Handling of information with very high protection needs in the context of *availability* (very high availability of information) Manejo de información con necesidad de protección muy alta en el contexto de la *disponibilidad* (disponibilidad muy alta de la información)

Núm.	Nombre	Descripción
7.	Proto parts	Protection of Prototype Parts and Components Protección de piezas y componentes prototipo
8.	Proto vehicles	Protection of Prototype Vehicles Protección de vehículos prototipo
9.	Test vehicles	Handling of Test Vehicles Manejo de vehículos de prueba
10.	Proto events	Protection of Prototypes during Events and Film or Photo Shoots Protección de prototipos durante eventos y rodajes o sesiones fotográficas
11.	Data	Data protection according to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR) Protección de datos en virtud del artículo 28 (“Encargado del tratamiento”) del Reglamento General de Protección de Datos europeo (RGPD)
12.	Special data	Data protection according to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR) with special categories of personal data as specified in Article 9 of the GDPR Protección de datos en virtud del artículo 28 (“Encargado del tratamiento”) del Reglamento General de Protección de Datos europeo (RGPD) con categorías especiales de datos personales como se define en el artículo 9 del RGPD

Tabla 3. Objetivos de evaluación TISAX actuales

Ejemplo: Si realiza recorridos de prueba con vehículos en la vía pública, el objetivo de evaluación “Test vehicles” será uno de sus objetivos de evaluación.

Recuerde:

Solo podrá seleccionar los objetivos de evaluación “Info high” e “Info very high” hasta el 31 de marzo de 2024.

Podrá seleccionar los objetivos de evaluación “Confidential” y “Strictly confidential” a partir del 1 de abril de 2024.

Para más información sobre este cambio, consulte el siguiente artículo de la

sección de noticias de nuestro sitio web:
CHANGES TO TISAX LABELS ACCOMPANYING ISA 6 RELEASE
enx.com/en-US/news/Changes-to-TISAX-Labels-ISA-six-Release/

Nota importante:

Dentro de TISAX, el “objetivo de evaluación” suele ser el punto de entrada del proceso. Sin embargo, algunos socios le pedirán que se someta a la evaluación TISAX según un “nivel de evaluación” (AL) determinado.

Para más información sobre la relación entre las necesidades de protección y los niveles de evaluación, consulte la Sección 4.3.3.5, “Necesidad de protección y niveles de evaluación”.

4.3.3.2. Objetivos de evaluación e ISA

La ISA contiene tres catálogos de criterios (seguridad de la información, protección de prototipos, protección de datos). Cada catálogo de criterios se compone de las llamadas “preguntas de control” y de los requisitos asociados.

Cada objetivo de evaluación define:

- el o los catálogos de criterios ISA aplicables
- las preguntas de control que debe responder
- los requisitos que debe cumplir

Para algunos objetivos de evaluación, solo se aplica un subconjunto de las preguntas de control y requisitos.

Para obtener más información sobre los objetivos de evaluación TISAX y las preguntas de control y requisitos aplicables, consulte la Sección 5.2.2, “Entender el documento ISA”.

4.3.3.3. Objetivos de evaluación y etiquetas TISAX

Puede que su socio le hable de las “etiquetas TISAX”. “Objetivos de evaluación” y “etiquetas TISAX” son casi lo mismo. La diferencia es que usted inicia el proceso de evaluación con los “objetivos de evaluación” y, si supera la evaluación, recibe las correspondientes “etiquetas TISAX”.

Ejemplo: Su socio le exige que obtenga la etiqueta TISAX “Info high”. En ese caso, ha de seleccionar “Info high” como objetivo de evaluación.

La siguiente figura muestra el punto de entrada y salida del proceso TISAX:

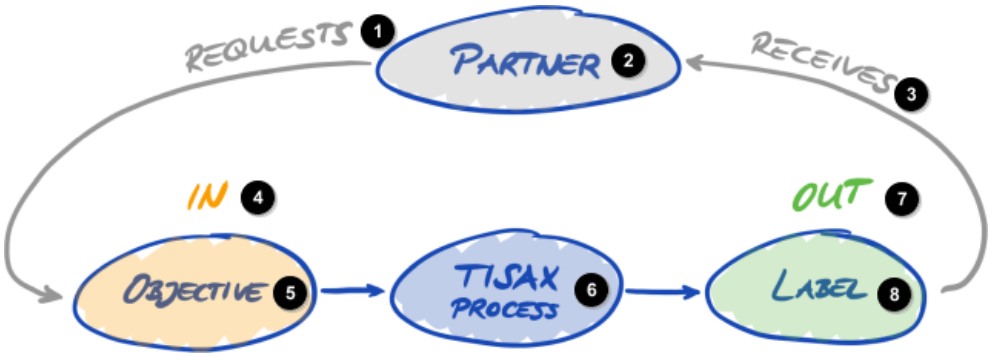


Figura 6. Objetivos de evaluación y etiquetas TISAX

1. Solicita
2. Socio
3. Recibe
4. ENTRADA
5. Objetivo
6. Proceso TISAX
7. SALIDA
8. Etiqueta

Para más información sobre las etiquetas TISAX, consulte la Sección 5.4.14, “Etiquetas TISAX”.

4.3.3.4. Selección de los objetivos de evaluación

Lo ideal es que su socio le diga exactamente qué objetivos de evaluación debe alcanzar.

Tendrá que seleccionar el objetivo de la evaluación a su propio juicio si:

a. quiere obtener la certificación TISAX antes de que un socio se la solicite, o
b. su socio no le dice qué objetivo de evaluación debe alcanzar.

Nota importante:

Llegados a este punto, le recomendamos que tenga en cuenta al resto de sus socios. ¿Tiene otros socios que exigen los mismos requisitos o similares? ¿Espera que sus socios futuros le exijan requisitos más altos?

Tal vez deba considerar seleccionar objetivos de evaluación con mayor necesidad de protección. De esta forma, se evitará problemas cuando otros socios tengan mayores requisitos.

Si ha de seleccionar el objetivo de evaluación a su propio juicio, tal vez le resulte útil tener en cuenta los siguientes aspectos:

Núm.	Objetivo de evaluación	Información
1.	Info high	Puede inferir la necesidad de protección (alta, muy alta) a partir de la clasificación de los documentos de su socio.
2.	Info very high	
3.	Confidential	Para todas las empresas que reciben y tratan información con necesidad de protección alta en el contexto de la confidencialidad o habitualmente clasificada como confidencial según el esquema de clasificación propio de la empresa (p. ej., el libro blanco de la VDA sobre armonización de niveles de clasificación). Debe seleccionar esta etiqueta TISAX especialmente si la divulgación no autorizada de la información pudiera ocasionar daños significativos (p. ej., daños a la reputación, consecuencias penales o perjuicios económicos).
4.	Strictly confidential	Para todas las empresas que reciben y tratan información con necesidad de protección muy alta en el contexto de la confidencialidad o habitualmente clasificada como estrictamente confidencial o secreta según el esquema de clasificación propio de la empresa (p. ej., el libro blanco de la VDA sobre armonización de niveles de clasificación). Debe seleccionar esta etiqueta TISAX especialmente si la divulgación no autorizada de la información pudiera ocasionar daños catastróficos o que atentan contra la existencia (p. ej., daños graves a la reputación, consecuencias penales graves o perjuicios económicos muy elevados).
5.	High availability	Para todas las empresas cuya capacidad de producción o de entrega de los clientes dependa de la disponibilidad de los productos o servicios de la empresa, y en las que un fallo causaría un daño considerable a los clientes en un corto periodo de tiempo. Ejemplo: proveedores «justo a tiempo» de material de producción

Núm.	Objetivo de evaluación	Información
6.	Very high availability	Para todas las empresas cuya capacidad de producción y de entrega de los clientes dependa de la disponibilidad a corto plazo de los productos o servicios de la empresa, y en las que un fallo causaría un gran daño a los clientes en un periodo de tiempo muy corto. Ejemplo: proveedores «justo a tiempo» en los que un fallo puede provocar, en un corto periodo de tiempo, una parada total de la producción con un tiempo de reanudación muy prolongado.
7.	Proto parts	Para todas las empresas que fabrican, almacenan o usan componentes o piezas suministradas por el cliente que requieren protección en sus propias ubicaciones. Los requisitos de seguridad física y del entorno, los requisitos organizativos y los requisitos especiales para la manipulación de prototipos son parte de la evaluación.
8.	Proto vehicles	Para todas las empresas que fabrican, almacenan o usan vehículos suministrados por el cliente que requieren protección en sus propias ubicaciones. Los requisitos de seguridad física y del entorno (incluida la existencia de garajes y zonas de taller con protección), los requisitos organizativos y los requisitos especiales para la manipulación de prototipos son parte de la evaluación. Tras superar la evaluación, automáticamente recibe la etiqueta TISAX “Protección de piezas y componentes prototipo”.

Núm.	Objetivo de evaluación	Información
9.	Test vehicles	Para todas las empresas que realizan pruebas y recorridos de prueba (p. ej., recorridos de prueba en la vía pública o en circuitos cerrados) con vehículos proporcionados por el cliente que requieren protección. Los requisitos organizativos y los requisitos específicos de la manipulación de prototipos, incluidos el camuflaje y la manipulación del vehículo durante los recorridos de prueba en la vía pública y en circuitos cerrados, son parte de la evaluación. Los requisitos de seguridad física y del entorno no son necesariamente parte de la evaluación. Si sus ubicaciones están equipadas en consecuencia, le recomendamos que también seleccione el objetivo de evaluación “Protección de vehículos prototipo”.
10.	Proto events	Para todas las empresas que llevan a cabo presentaciones o eventos (p. ej., estudios de mercado, eventos, eventos de marketing) y rodajes o sesiones fotográficas con vehículos proporcionados por el cliente que requieren protección. Los requisitos organizativos y los requisitos específicos de la manipulación de prototipos, incluidos los requisitos para presentaciones, eventos, rodajes y sesiones fotográficas en espacios protegidos o en público, son parte de la evaluación. Los requisitos de seguridad física y del entorno no son necesariamente parte de la evaluación. Si sus ubicaciones están equipadas en consecuencia, le recomendamos que también seleccione el objetivo de evaluación “Protección de vehículos prototipo”.
11.	Data	Si trata datos personales como encargado del tratamiento según el artículo 28 del RGPD, seguramente deberá seleccionar “Data”.

Núm.	Objetivo de evaluación	Información
12.	Special data	Si trata categorías especiales de datos personales (como datos sobre salud o religión) como encargado del tratamiento según el artículo 28 del RGPD, seguramente deberá seleccionar “Special data”.

Tabla 4. Consejos para seleccionar el objetivo de evaluación

Explicaciones adicionales:

- Si tiene requisitos precisos de su socio, normalmente no tendrá que discutir los objetivos de evaluación con este. No obstante, si no tiene requisitos precisos por parte del socio, le recomendamos que lo consulte con él antes de empezar el proceso de evaluación.
- La ISA describe la diferencia de implementación entre necesidad de protección “alta” y “muy alta” (si la hay) para cada requisito.
  Para más información al respecto, consulte la Figura 11, “Captura de pantalla: Elementos principales de las preguntas en el catálogo de criterios ISA “Seguridad de la información””.

4.3.3.5. Necesidad de protección y niveles de evaluación

Su socio tiene varios tipos de información, de los cuales algunos necesitan un nivel de protección más alto que otros. La ISA lo contempla diferenciando tres “necesidades de protección” (“protection needs”): normal, alta y muy alta. Su socio clasifica la información y habitualmente asigna necesidades de protección.

Cuanto mayores sean las necesidades de protección, más interés tendrá el socio en asegurarse de que es seguro dejarle manejar su información. Por tanto, TISAX diferencia tres “niveles de evaluación” (AL). El nivel de evaluación define qué método de evaluación debe aplicar el proveedor de auditoría. Un nivel de evaluación más alto aumenta el esfuerzo dedicado a la evaluación. El resultado es un mayor cuidado y precisión en la evaluación.

La siguiente tabla muestra los niveles de evaluación que se aplican a los objetivos de evaluación TISAX:

Núm.	Objetivo de evaluación TISAX	Nivel de evaluación (AL)
1.	Info high	AL 2
2.	Info very high	AL 3
3.	Confidential	AL 2
4.	Strictly confidential	AL 3
5.	High availability	AL 2

Núm.	Objetivo de evaluación TISAX	Nivel de evaluación (AL)
6.	Very high availability	AL 3
7.	Proto parts	AL 3
8.	Proto vehicles	AL 3
9.	Test vehicles	AL 3
10.	Proto events	AL 3
11.	Data	AL 2
12.	Special data	AL 3

Tabla 5. Asignación de los objetivos de evaluación TISAX a los niveles de evaluación

Nivel de evaluación 1 (AL 1):

Las evaluaciones en el nivel de evaluación 1 son principalmente para fines internos en el sentido de una autoevaluación (self-assessment).

En las evaluaciones del nivel de evaluación 1, el auditor comprueba la existencia de una autoevaluación completada. No evalúa el contenido de la autoevaluación. No exige más evidencias.

Los resultados de las evaluaciones en el nivel de evaluación 1 tienen un nivel de confianza bajo y por eso no se usan en TISAX. Pero, lógicamente, es posible que su socio le solicite una autoevaluación de este tipo fuera de TISAX.

Nivel de evaluación 2 (AL 2):

Para una evaluación dentro del nivel de evaluación 2, el proveedor de auditoría lleva a cabo una comprobación de plausibilidad de su autoevaluación (para todas las ubicaciones dentro del alcance de la evaluación). Lo hace comprobando las evidencias[8] y entrevistando a la persona encargada de la seguridad de la información.

El proveedor de auditoría acostumbra a realizar esta entrevista por videoconferencia. Si usted lo solicita, puede realizar la entrevista en persona.

Si tiene evidencias que no quiere enviar al proveedor de auditoría, puede solicitar una inspección in situ. De esta forma, el proveedor de auditoría podrá comprobar esa evidencia ante usted con la máxima confidencialidad.

Recuerde:

> Existe un método alternativo para realizar una evaluación en el nivel de evaluación 2. En lugar de la comprobación de plausibilidad, el proveedor de auditoría lleva a cabo una evaluación remota completa. Este método se denomina a veces “**nivel de evaluación 2.5**”.
>
> En comparación con una evaluación en el nivel de evaluación 2, el auditor *verifica* si su ISMS cumple los requisitos aplicables. Sin embargo, a diferencia de una evaluación en el nivel de evaluación 3, el auditor no lleva a cabo las actividades in situ que se describen en la sección sobre el nivel de evaluación 3.
>
> Formalmente, dicha evaluación se valorará como una evaluación en el AL 2.
>
> La ventaja del AL 2.5 es que el enfoque es metódicamente compatible con el AL 3. Por lo tanto, permitirá pasar más adelante a una evaluación completa en el AL 3 con un esfuerzo asumible. Para ello, el auditor solo tiene que llevar a cabo las actividades in situ descritas en la sección sobre el AL 3.
>
> Recomendamos evaluaciones en el nivel de evaluación 2.5 en estos casos:
>
> 1. Actualmente solo necesita etiquetas TISAX que impliquen una evaluación en el AL 2, pero no puede excluir la posibilidad de que otros socios requieran más adelante etiquetas TISAX que impliquen una evaluación en el AL 3. Una evaluación en el AL 2.5 mantiene las puertas abiertas a una posterior ampliación al AL 3.
> 2. Tiene dificultades para elaborar una autoevaluación suficientemente plausible. Para la comprobación de plausibilidad, la autoevaluación tiene que ser concluyente, bien comprensible y estar documentada. Elaborar una autoevaluación de este tipo puede suponer un esfuerzo interno considerable, incluso para las empresas que están bien posicionadas.
>
> Para más información sobre cómo ampliar el nivel de evaluación, consulte la Sección 7.10, “Anexo: Evaluación de la ampliación del alcance”.
>
> Esta alternativa es opcional y no es necesaria para cumplir los requisitos del AL 2. La diferencia entre el AL 2 y el AL 2.5 no será visible para los socios con los que comparta el resultado de su evaluación.

Nivel de evaluación 3 (AL 3):

Para una evaluación dentro del nivel de evaluación 3, el proveedor de auditoría lleva a cabo una verificación completa del cumplimiento de todos los requisitos aplicables por parte de su empresa. El auditor utiliza su autoevaluación y la documentación presentada para preparar la evaluación. Pero, a diferencia del nivel de evaluación 2, el auditor lo verificará todo. Esto incluye:

- examinar documentos y pruebas
- realizar entrevistas programadas con los propietarios de los procesos
- observar las condiciones locales
- observar la ejecución de los procesos
- realizar entrevistas *no* programadas con participantes en los procesos

Recuerde:

El texto siguiente hace referencia a varios conceptos que se explicarán más adelante en este documento.

Con el AL 3, el proveedor de auditoría debe desplazarse a sus ubicaciones. Si esto no fuera posible temporalmente por alguna razón o requiriera un esfuerzo excesivo, su proveedor de auditoría puede utilizar el **método de evaluación a distancia asistido por vídeo** para llevar a cabo las actividades in situ de la evaluación.

Su proveedor de auditoría deberá registrarlo en el informe de evaluación TISAX como una no conformidad menor. Tan pronto como su proveedor de auditoría pueda acudir a su ubicación, deberá realizar una evaluación de seguimiento que incluya todas las actividades in situ que no se habían podido realizar. Además, tiene que programar la evaluación de seguimiento aunque aún no haya completado las demás acciones correctivas.

En comparación con esperar a que su proveedor de auditoría esté disponible para las actividades in situ, este enfoque le permite compartir ya etiquetas TISAX temporales con su socio.

Niveles de evaluación y métodos de evaluación

La siguiente tabla proporciona un resumen simplificado de los métodos de auditoría asociados a cada nivel de evaluación:

Método de evaluación	Nivel de evaluación 1 (AL 1)	Nivel de evaluación 2 (AL 2)	Nivel de evaluación 3 (AL 3)
Autoevaluación	Sí	Sí	Sí
Evidencia	No	Comprobación de plausibilidad	Verificación exhaustiva
Entrevistas	No	Por videoconferencia[9]	En persona, in situ

Método de evaluación	Nivel de evaluación 1 (AL 1)	Nivel de evaluación 2 (AL 2)	Nivel de evaluación 3 (AL 3)
Inspección in situ	No	Si lo solicita	Sí

Tabla 6. Aplicabilidad de los métodos de evaluación a los distintos niveles de evaluación

Información adicional:

- Diferencia entre AL 2 y AL 3
  Metodológicamente, los dos enfoques se diferencian bastante. En el caso de las evaluaciones en el nivel de evaluación{npsp}2, el auditor no verificará todo. Solo comprobará la plausibilidad. Por lo tanto, el proveedor de auditoría no puede utilizar los resultados de una evaluación en el nivel de evaluación 2 como base para una ampliación al nivel de evaluación 3. Los esfuerzos necesarios para una actualización al nivel de evaluación 3 son prácticamente los mismos que para una nueva evaluación inicial.
- Comprobación de plausibilidad frente a verificación
  Simplificando mucho, una comprobación de plausibilidad es comprobar si algo existe y *parece* correcto. Por el contrario, una verificación significa comprobar realmente que algo es lo que dice ser.
- Clasificación de la información y necesidades de protección
  La asignación de la clasificación de la información (como confidencial o secreta) a las necesidades de protección puede ser diferente para distintos socios. Por tanto, por mucho que quisiéramos, no podemos proporcionar una tabla simple en la que la clasificación de la información de su socio se corresponda exactamente con una necesidad de protección.
- Saber el nivel de evaluación no es suficiente
  Algunos socios pueden exigir la evaluación TISAX según un nivel de evaluación determinado. Sin embargo, entienda que conocer el nivel de evaluación no es suficiente para iniciar el proceso TISAX. Un nivel de evaluación solo tiene sentido en combinación con un catálogo de criterios ISA y una necesidad de protección. Habitualmente, los socios piden que se obtenga una etiqueta TISAX (catálogo de criterios más necesidad de protección) No obstante, como las necesidades de protección equivalen a los niveles de evaluación, sí es suficiente si conoce el catálogo de criterios y el nivel de evaluación.
- Jerarquía de los niveles de evaluación
  Los niveles de evaluación superiores siempre incluyen los niveles de evaluación inferiores. Por ejemplo, si su evaluación se basa en el nivel de evaluación 3, automáticamente cumplirá todos los requisitos del nivel de evaluación 2.
- Nuestro consejo en materia de niveles de evaluación
  Si ha seleccionado un objetivo de evaluación (y, con ello, el correspondiente nivel de evaluación) a su propio juicio, le recomendamos que seleccione objetivos de evaluación que impliquen un nivel de evaluación 3. El esfuerzo requerido para una evaluación TISAX en el nivel de evaluación 3 no suele ser mayor al requerido en el nivel de evaluación 2.

Los proveedores que tienen varios socios, a menudo seleccionan objetivos de evaluación que implican el nivel de evaluación 3. De esta forma, están preparados para todas las exigencias futuras y no tienen que preocuparse por los distintos niveles de evaluación.

- Otras consideraciones comerciales
  En lo referente a los niveles de evaluación, el coste total de una evaluación TISAX es la suma del esfuerzo interno y del coste de la evaluación. Mientras que el coste de una evaluación en el nivel de evaluación 2 es inferior, el esfuerzo interno puede ser mayor. Esto se debe a que una evaluación en el nivel de evaluación 2 a menudo exige una autoevaluación más amplia y mejor documentación interna. Para las evaluaciones en el nivel de evaluación 3, mostrar cómo hace las cosas y presentar documentación básica suele ser evidencia suficiente para el auditor. Pero, sin una inspección in situ, el auditor le pedirá documentación muy precisa. Por tanto, es bastante frecuente optar por el nivel de evaluación 3 en lugar del nivel de evaluación 2. De todos modos, es una elección más habitual en las empresas pequeñas que en las grandes.

4.3.3.6. Objetivos de evaluación y sus propios proveedores

TISAX no exige que aplique los mismos requisitos a todos sus proveedores. Si su objetivo de evaluación es “Seguridad de la información con necesidad de protección *muy* alta”, esto NO significa automáticamente que sus propios proveedores deban alcanzar el mismo objetivo de evaluación. Ni siquiera significa que deban tener etiquetas TISAX.

Pero tendrá que comprobar para todos sus proveedores si usar sus servicios aumenta los riesgos o implica nuevos riesgos.

Dos ejemplos simplificados:

1. Según su política, el correo electrónico convencional no se puede utilizar para datos con necesidad de protección muy alta. Por tanto, su proveedor de correo electrónico no necesita obtener la etiqueta TISAX con necesidad de protección muy alta.
   También puede llegar a la misma conclusión si únicamente envía mensajes de correo electrónico cifrados y su proveedor de correo electrónico no puede ver los datos con necesidad de protección muy alta.
2. Usted elimina los datos impresos con necesidad de protección muy alta mediante una trituradora de papel. En ese caso, lógicamente, su proveedor de recogida de residuos no está obligado a cumplir los mismos requisitos que usted.

No obstante, una evaluación del riesgo podría mostrar que su proveedor también debe cumplir los requisitos para la necesidad de protección muy alta. En ese caso, las etiquetas TISAX son una opción para acreditarlo.

4.3.4. Tasa

Cobramos una tasa. Nuestra lista de precios informa de las tasas aplicables, los posibles

descuentos y las condiciones de pago.

Puede descargar la lista de precios en nuestro sitio web en:
enx.com/en-US/TISAX/downloads/
Descarga directa en PDF:
enx.com/pricelist.pdf

Existen algunos aspectos relacionados con la facturación que deberá tener en cuenta durante los preparativos para el registro:

- Selección de la dirección de facturación
  De forma predeterminada, enviaremos la factura a la dirección que haya indicado como ubicación del participante. Sin embargo, puede proporcionar una dirección diferente para recibir la factura.

Nota importante:

Asegúrese de que la dirección de facturación es correcta. Las leyes sobre contabilidad requieren que la dirección en nuestra factura coincida exactamente con la dirección (de facturación) de su empresa. Por razones legales, no podemos cambiar la dirección de una factura una vez que la hemos emitido.

- Referencia de pedido
  Si necesita ver un número de pedido específico o algo similar en su factura, podrá proporcionarnos una referencia de pedido.
- NIF-IVA
  Todos nuestros cargos están sujetos al impuesto sobre el valor añadido (IVA) alemán (si procede).
  Necesitamos este número para procesar los pagos de la UE. Es obligatorio proporcionar un NIF-IVA si la dirección de facturación está en alguno de los siguientes países:
  Alemania, Austria, Bélgica, Bulgaria, Croacia, Chipre (parte griega), Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Suecia, Reino Unido, República Checa
- Gestión de proveedores

Nota importante:

Entienda que, dada la reciprocidad entre todos los participantes de TISAX, no podemos aceptar condiciones generales adicionales (como condiciones generales de compraventa o códigos de conducta).

Información adicional sobre nuestro proceso de facturación:

- No podemos aceptar condiciones de compra individuales.
- Aceptamos:
  - transferencias a la cuenta bancaria especificada en la factura
  - pagos con tarjeta de crédito (durante el proceso de registro a través de nuestro proveedor de servicios de pago “Stripe”)
- Nuestra factura incluirá las siguientes referencias a su registro:
  - El nombre y la dirección de correo electrónico de la persona de contacto principal del participante
  - El nombre del alcance de la evaluación

  Encontrará un ejemplo de factura en el anexo, en la Sección 7.1, “Anexo: Ejemplo de factura”.
- La mayoría de datos que pueda necesitar para procesar la factura estarán incluidos en la misma. Estos y otros datos están disponibles en nuestro documento “Information for Members and Business Partners” (Información para miembros y socios comerciales). Envíenos un mensaje de correo electrónico y le haremos llegar la versión actual.

Recuerde:

Somos conscientes de que el proceso de aprobación interno de pagos en algunas empresas requiere cierto tiempo. Por ese motivo, sus siguientes pasos inmediatos del proceso TISAX no dependen de que recibamos el pago. Sin embargo, tenga en cuenta que no podrá compartir el resultado de la evaluación hasta que no hayamos recibido el pago.
Por ese motivo, le recomendamos que se asegure de enviar la factura al destinatario adecuado y de que contenga una referencia de pedido en caso aplicable. También puede hacer un seguimiento interno del pago de la factura.

Nota importante:

Nosotros --ENX Association-- facturamos la tasa. Esta tasa es solo una parte del coste total de una evaluación TISAX. Su proveedor de auditoría TISAX facturará el coste de la evaluación o las evaluaciones.

Para más información sobre los costes relacionados con el proveedor de auditoría, consulte la Sección 5.3.4, “Valoración de las ofertas”.

Nota importante:

Deberá pagar la tasa independientemente de que:

- continúe o no con el proceso TISAX.
- supere con éxito el proceso de evaluación TISAX.

Por tanto, es posible que la factura le llegue antes de que empiece la evaluación inicial.

4.4. Portal ENX

La siguiente sección describe el proceso de registro online en el que introduce todos los datos recopilados siguiendo las indicaciones de la sección anterior. Antes de iniciar el proceso de registro online, permítanos explicarle brevemente la finalidad y las ventajas del portal ENX.

El portal ENX nos permite mantener una base de datos de todos los participantes de TISAX y desempeña un papel importante a lo largo de todo el proceso TISAX. Durante el registro TISAX, usted introduce datos que los proveedores de auditoría TISAX pueden usar (si así lo autoriza) para calcular su oferta y planificar el procedimiento de evaluación. Una vez que lleve a cabo el proceso de evaluación TISAX, usará la plataforma de intercambio en el portal ENX para compartir el resultado de la evaluación con su socio.

El nombre del portal es “portal ENX” en lugar de “portal TISAX” porque también lo usamos para gestionar otras actividades empresariales (como la red ENX).

4.5. Proceso de registro online

Si se ha preparado según las indicaciones anteriores (Sección 4.3, “Preparación del registro”), estará listo para iniciar el proceso de registro online.

4.5.1. Tiempo necesario

El tiempo necesario depende en gran medida del número de alcances y ubicaciones que registre. Para su primer registro como participante con un alcance y una ubicación, cuente con un mínimo de 20 minutos.

Recomendamos que complete el registro en una sola sesión, porque actualmente no se pueden recuperar algunos pasos más tarde. En caso de que necesite pausar el proceso, nos pondremos en contacto con usted para obtener cualquier dato que falte.

4.5.2. Empiece aquí

Inicie el registro en nuestro sitio web en:
enx.com/en-us/Account/Login/Register?returnUrl=%2FTISAX%2Ftisax-initial-registration%2F

Básicamente, todo lo que tiene que hacer es seguir las instrucciones que aparecen en pantalla. No obstante, a continuación describimos el proceso brevemente.

4.5.3. Cuenta en el portal

El primer paso es crearse una cuenta en el portal ENX. Necesitará la cuenta en el portal para poder gestionar los “datos de participante” de su empresa.

Recuerde:

Si el portal ENX le indica que su dirección de correo electrónico ya está en uso, póngase en contacto con nosotros. Este mensaje puede indicar que, por algún motivo, su nombre ya está registrado en nuestro sistema.

Recuerde:

Como se ha descrito, las cuentas del portal no son necesariamente “contactos del participante” o “contactos del alcance” (vea más abajo) con un rol activo en el proceso de evaluación.

Y viceversa, un “contacto del participante” o “contacto del alcance” no incluye automáticamente los mismos derechos para gestionar los datos del participante que con una cuenta del portal. Es decir, los empleados designados como “contacto del participante” o “contacto del alcance” no puede acceder automáticamente a los datos del participante en el portal ENX.

Si quiere asignar el derecho de gestionar los datos del participante a un contacto que ya ha creado en el portal ENX (independientemente de si le asignó un rol), debe invitar al contacto. Para más información, consulte la última nota en la Sección 4.5.5, “Contacto del participante”.

4.5.4. Registro como participante

El segundo paso es registrar su empresa como participante de TISAX. El “participante de TISAX” es la empresa que intercambiará los resultados de la evaluación con otros participantes.

4.5.5. Contacto del participante

En general, será la persona responsable en su empresa para todos los temas relacionados con la evaluación de la seguridad de la información. Puede ser usted u otra persona de su empresa.

Normalmente, todo lo que necesitamos es el contacto principal del participante. Sin embargo, si prefiere que todas las comunicaciones que enviemos nosotros y los proveedores de auditoría TISAX en el contexto de este registro lleguen también a otras personas, añada contactos del participante adicionales.

Nota importante:

Recomendamos asignar al menos un sustituto para cada contacto. Si un contacto no está disponible temporalmente o abandona la empresa, otra persona podrá gestionar los datos de participante de su empresa.
Si necesita asignar un nuevo contacto (sin tener ningún otro contacto válido), deberá seguir un proceso complejo. Nuestro proceso asegura que solo las personas que pueden demostrar que están autorizadas a representar legalmente a la empresa puedan aprobar la asignación de un nuevo contacto principal.

Recuerde:

Siempre podrá añadir o eliminar contactos más adelante (incluso tras haber completado el proceso de registro online e incluso después de haber finalizado la evaluación).

Recuerde:

No puede usar direcciones de correo electrónico genéricas para los contactos del participante (como “info@acme.com” o “IT@acme.com”).

Esta regla es conforme con los requisitos ISA sobre el registro de usuarios.

Recuerde:

Puede elegir si cada contacto debe tener acceso a los datos de participante de su empresa. O bien:

1. Solo añade el contacto. El contacto se almacena en nuestro sistema pero no puede iniciar sesión ni gestionar datos.
2. O invita al contacto. En ese caso, el portal ENX envía una invitación al contacto por correo electrónico. El contacto debe seguir el enlace de invitación que figura en el mensaje de correo electrónico. Una vez que el contacto ha creado su propia cuenta personal para el portal ENX, podrá gestionar los datos de participante de su empresa.

Para crear un nuevo contacto: Inicio de sesión > MY TISAX (MI TISAX) > ADMINISTRATORS (ADMINISTRADORES) > Create new TISAX Administrator (Crear nuevo administrador TISAX)

Para invitar a un contacto: Inicio de sesión > MY TISAX (MI TISAX) > ADMINISTRATORS (ADMINISTRADORES) > Vaya al final de la fila de la tabla del contacto y haga clic en el botón con la flecha hacia abajo > Edit TISAX Administrator (Editar administrador TISAX) > Vaya al apartado “ENX PORTAL ACCESS” (ACCESO AL PORTAL ENX) > Ajuste “INVITE THIS CONTACT” (INVITAR

A ESTE CONTACTO) a “Yes” (Sí) > Haga clic en “Save Contact” (Guardar contacto)

4.5.6. Condiciones generales

El tercer paso es aceptar las “TISAX Participation General Terms and Conditions” (Condiciones generales de participación en TISAX).

Puede volver a consultar las notas explicativas en la Sección 4.3.1, “La base legal”.

4.5.7. Registro del alcance de la evaluación

El cuarto paso es registrar el alcance de la evaluación para su evaluación de la seguridad de la información.

Le pedimos que:

1. asigne un nombre al alcance de la evaluación.
   La finalidad principal del nombre del alcance es facilitarle la identificación del alcance en la lista general de alcances del portal ENX.
   Puede volver a consultar las notas explicativas en la Sección 4.3.2.6, “Nombre del alcance”
2. elija un tipo de alcance de la evaluación.
   (Estándar, personalizado)
   Puede volver a consultar las notas explicativas en la Sección 4.3.2, “El alcance de la evaluación TISAX”.
3. especifique el contacto principal del alcance.
   Será la persona generalmente responsable de la evaluación de un alcance en particular.
   Puede ser usted u otra persona de su empresa.
   Normalmente, todo lo que necesitamos es el contacto principal del alcance. Sin embargo, si prefiere que todas las comunicaciones que enviemos nosotros en el contexto de este alcance lleguen también a otras personas, puede añadir contactos del participante adicionales.
4. seleccione el o los objetivos de la evaluación.
   Puede volver a consultar las notas explicativas en la Sección 4.3.3, “Objetivos de evaluación”.
5. añada la o las ubicaciones del alcance de la evaluación.
   Le pedimos que especifique todas las ubicaciones que forman parte del alcance de la evaluación.
   Puede volver a consultar las notas explicativas en la Sección 4.3.2, “El alcance de la evaluación TISAX”.

Recuerde:

Una vez que haya creado una ubicación, ya no podrá editarla. Para cambios menores (cambio del nombre de la empresa, erratas en el nombre de la

calle, el código postal, la localidad, etc.), póngase en contacto con nosotros. Nosotros lo editaremos.

Nota importante:

Esta nota solo es relevante si está renovando las etiquetas TISAX.

Vuelva a utilizar los registros de ubicación existentes que creó y utilizó durante el registro de su alcance anterior. No cree un nuevo registro de ubicación con la misma dirección.

Motivo: Algunos participantes de TISAX procesan los resultados de evaluación de sus socios automáticamente. A tal fin, sincronizan su propio sistema con el portal ENX. Incluso las diferencias más insignificantes pueden provocar un fallo de sincronización. Además, no debería recargar sus datos de participante con duplicados innecesarios.

6. seleccione los niveles de publicación y divulgación (opcional).
   Puede decidir ya si quiere publicar el resultado de la evaluación para otros participantes de TISAX y compartirlo con su(s) socio(s). Lo normal es permitir que mostremos que su empresa es un participante y que ha superado con éxito el proceso TISAX.
   Puede saltar sin problemas este paso durante su registro inicial. Siempre puede definir el acceso al resultado de su evaluación más tarde.
   Puede volver a consultar las notas explicativas en la Sección 4.3.2.8, “Publicación y divulgación”.

Nota importante:

No puede revocar los permisos de publicación o divulgación.
Para más información, consulte la Sección 6.4, “Permanencia de los resultados intercambiados”.

7. especifique quién recibe la factura.
   Le pedimos que especifique quién recibirá nuestra(s) factura(s).
   Puede volver a consultar las notas explicativas en la Sección 4.3.4, “Tasa”.

Recuerde:

No puede equivocarse mucho aquí. Si más tarde descubre que debería haber registrado un alcance ligeramente diferente (ha olvidado una ubicación, tiene otro objetivo de evaluación, etc.), el proveedor de auditoría podrá realizar la evaluación de todos modos.

Ejemplo: El auditor determina que el ámbito debe contener una ubicación adicional que usted no añadió originalmente al alcance. El auditor llevará a cabo la auditoría y posteriormente actualizará el alcance de su evaluación en el portal ENX cuando cargue el resultado de su evaluación.

Recuerde:

Cada alcance de la evaluación tiene un ciclo de vida. Llegados a este punto, el alcance de la evaluación tiene el estado “Incompleto”, “Pendiente del pedido” o “Pendiente de aprobación”.

Para más información sobre el estado de un alcance de la evaluación, consulte la Sección 7.5.1, “Sinopsis: Assessment scope status (Estado del alcance de la evaluación)”.

Recuerde:

Para las empresas grandes con muchas ubicaciones, TISAX ofrece la evaluación en grupo simplificada. Puede plantearse esta opción si:

- tiene al menos tres ubicaciones en su alcance[10] y
- si su sistema de gestión de la seguridad de la información está organizado de forma centralizada y a punto[11].

Para una evaluación en grupo simplificada, el esfuerzo inicial es mayor. No obstante, se compensa cuantas más ubicaciones tenga.

Para más información sobre la “evaluación en grupo simplificada”, consulte el documento “TISAX Simplified Group Assessment” (Evaluación en grupo simplificada TISAX).

Puede descargar el documento “TISAX Simplified Group Assessment” en nuestro sitio web en:
enx.com/en-US/TISAX/downloads/

Descarga directa en PDF:
enx.com/sga.pdf

Recuerde:

Una vez registrado el alcance de la evaluación, ya no podrá cambiarlo usted mismo.

Si puede asegurar de forma fehaciente que todavía NO ha enviado su “TISAX

Scope Excerpt" a nuestros proveedores de auditoría, póngase en contacto con nosotros. Lo cambiaremos por usted.

Si ya ha enviado su "TISAX Scope Excerpt" a (uno de) nuestros proveedores de auditoría, deberá simplemente crear la nueva ubicación en el portal ENX (si procede) y discutir los posibles cambios con el proveedor de auditoría. Su proveedor de auditoría llevará a cabo la evaluación basándose en los cambios y actualizará la información sobre el alcance en el portal ENX.

Recuerde:

Usted no puede borrar un alcance de evaluación en el portal ENX. Si ha creado un alcance de evaluación por error, póngase en contacto con nosotros. Lo borraremos por usted.

4.5.8. Mensaje de correo electrónico de confirmación

Una vez que haya completado los pasos obligatorios anteriores, comprobaremos su solicitud. A continuación, le enviaremos un mensaje de correo electrónico de confirmación.

Este mensaje de correo electrónico tiene dos elementos importantes:

- Una lista de contacto con todos los proveedores de auditoría TISAX
  Deberá elegir uno de nuestros proveedores de auditoría TISAX para llevar a cabo la evaluación de su alcance. Puede usar los contactos para solicitar ofertas.
  Para más información sobre la selección del proveedor de auditoría, consulte la Sección 5.3, "Selección del proveedor de auditoría".
- El "TISAX Scope Excerpt" como archivo PDF adjunto

  Contiene:

  - La información que hemos almacenado en nuestra base de datos
  - Su ID de participante
    Consulte la Sección 4.5.8.1, "Participant ID (ID de participante)" más abajo.
  - Su(s) ID de alcance
    Consulte la Sección 4.5.8.2, "Scope ID (ID de alcance)" más abajo.

Para ver un ejemplo de nuestro mensaje de correo electrónico de confirmación, consulte la Sección 7.2, "Anexo: Ejemplo de mensaje de correo electrónico de confirmación".

Para ver un ejemplo del "TISAX Scope Excerpt", consulte la Sección 7.3, "Anexo: Ejemplo de TISAX Scope Excerpt".

Por norma general, recibirá nuestro mensaje de confirmación en un plazo de tres días hábiles.

Si no tiene noticias nuestras en un plazo de siete días laborables, compruebe que a) ha facilitado toda la información y b) el estado del alcance de la evaluación es “Awaiting ENX approval” (Pendiente de aprobación ENX). Solo empezaremos a procesar su registro cuando todo esté completo. Si cree que todo está completo, pero no nos hemos puesto en contacto con usted, póngase en contacto con nosotros.

Enviamos nuestro mensaje de confirmación al contacto principal del participante.

Recuerde:

Cada alcance de la evaluación tiene un ciclo de vida. Llegados a este punto, su alcance de la evaluación tiene el estado “Awaiting ENX approval” (Pendiente de aprobación ENX).

Para más información sobre el estado de un alcance de la evaluación, consulte la Sección 7.5.5, “Assessment scope status “Awaiting your payment” (Estado del alcance de la evaluación “Pendiente de pago”)”.

Las dos subsecciones siguientes proporcionan información detallada sobre la finalidad de su ID de participante e ID de alcance.

4.5.8.1. Participant ID (ID de participante)

El ID de participante:

- identifica a un participante de TISAX.
- es único para cada participante.
- se asigna una vez completado el registro.
- es un requisito previo para pedir una evaluación de la seguridad de la información a cualquiera de nuestros proveedores de auditoría TISAX.
- tiene esta estructura:

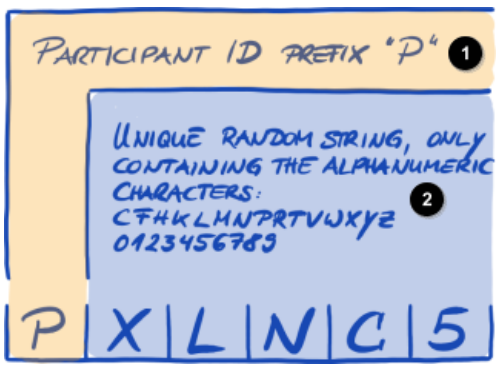


Figura 7. Formato del ID de participante[12]

1. Prefijo “P” del ID de participante
2. Secuencia aleatoria única, compuesta solo por los caracteres alfanuméricos:
   CFHKLMNPRTVWXYZ
   0123456789

Recuerde:

Hay dos formas de encontrar el ID de participante:

1. Compruebe su “TISAX Scope Excerpt”.
   Consulte la Sección 4.5.8, “Mensaje de correo electrónico de confirmación” más arriba.
2. Inicie sesión en el portal ENX, vaya a la barra de navegación principal y seleccione “DASHBOARD” (“PANEL”). Allí encontrará su ID de participante.

4.5.8.2. Scope ID (ID de alcance)

El ID de alcance:

- identifica un alcance de la evaluación.
- es único para cada alcance de la evaluación.
- se asigna una vez completado el registro.
- es un requisito previo para que pueda pedir una evaluación de la seguridad de la información a cualquiera de nuestros proveedores de auditoría TISAX.
- tiene esta estructura:

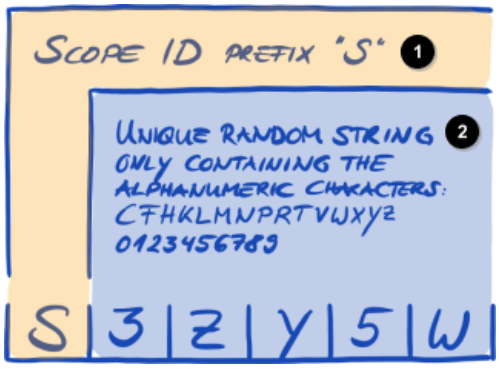


Figura 8. Formato del ID de alcance

1. Prefijo “S” del ID de alcance

2 Secuencia aleatoria única, compuesta solo por los caracteres alfanuméricos:
CFHKLMNPRTVWXYZ
0123456789

Recuerde:

Hay dos formas de encontrar el ID de alcance:

1. Compruebe su “TISAX Scope Excerpt”.
   Consulte la Sección 4.5.8, “Mensaje de correo electrónico de confirmación” más arriba.
2. Inicie sesión en el portal ENX, vaya a la barra de navegación principal, seleccione “MY TISAX” (MI TISAX) y, a continuación, “SCOPES AND ASSESSMENTS” (ALCANCES Y EVALUACIONES). Allí encontrará su(s) ID de alcance.

Recuerde:

Cada alcance de la evaluación (identificado por su ID de alcance) tiene un ciclo de vida.

Para más información sobre el estado de un alcance de la evaluación, consulte la Sección 7.5, “Anexo: Assessment scope status (Estado del alcance de la evaluación)”.

4.5.9. Información de estado

Llegados a este punto, hay dos estados relevantes para describir su posición en el proceso TISAX:

1. Estado del participante
2. Estado del alcance de la evaluación

El siguiente diagrama ilustra las condiciones que deben cumplirse para alcanzar un determinado estado:

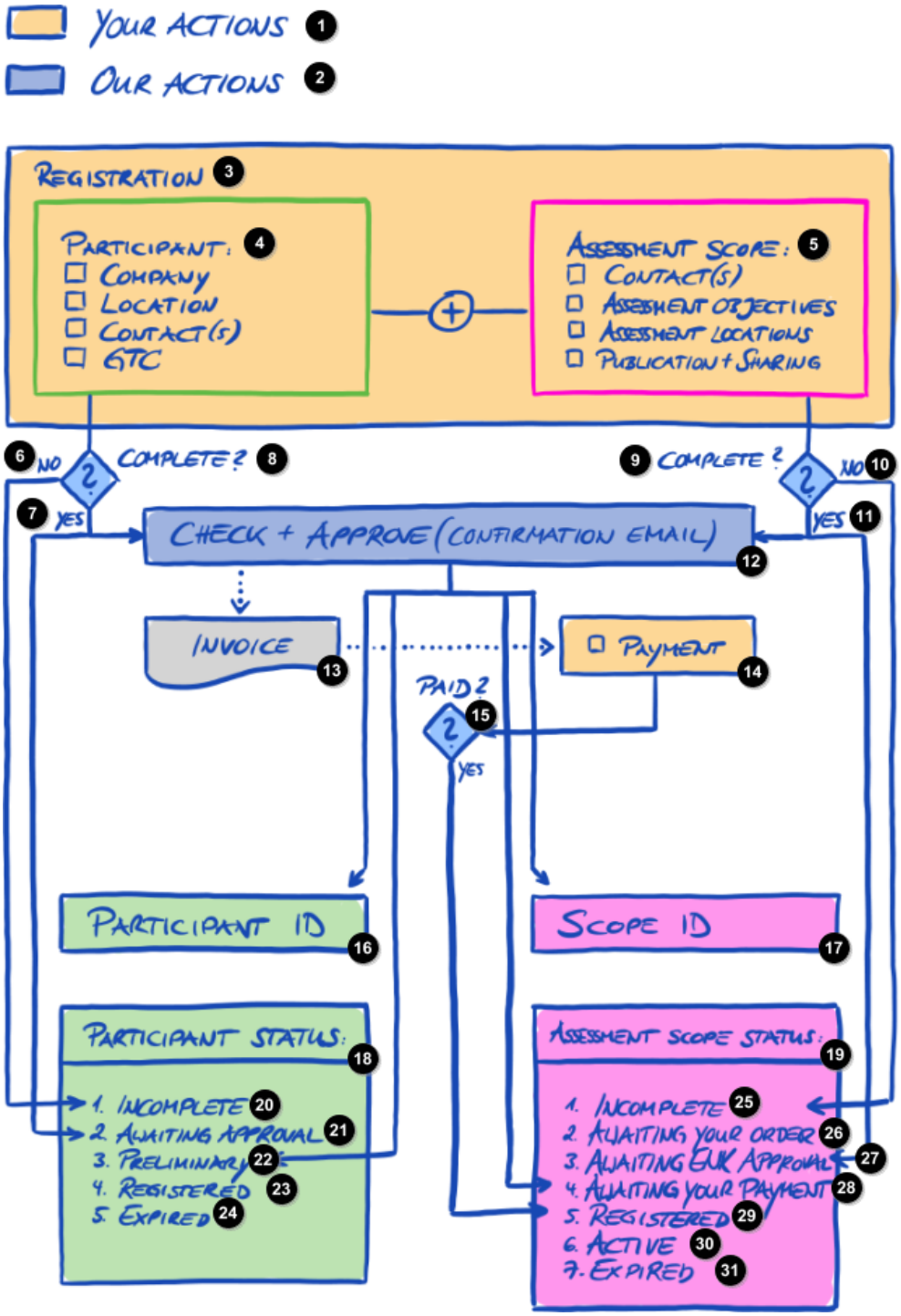


Figura 9. Condiciones para el estado del participante y el estado del alcance de la evaluación

1. Sus acciones
2. Nuestras acciones
3. Registro

4. Participante:
[ ] Empresa
[ ] Ubicación
[ ] Contacto(s)
[ ] Condiciones generales

5. Alcance de la evaluación:
[ ] Contacto(s)
[ ] Objetivos de evaluación
[ ] Ubicaciones de la evaluación
[ ] Publicación + divulgación

6. No

7. Sí

8. ¿Completo?

9. ¿Completo?

10. No

11. Sí

12. Comprobación + aprobación (mensaje de confirmación)

13. Factura

14. [ ] Pago

15. ¿Pagado?

16. ID de participante

17. ID de alcance

18. Estado del participante:

19. Estado del alcance de la evaluación:

20. 1. Incompleto

21. 2. Pendiente de aprobación

22. 3. Preliminar

23. Registrado

24. Expirado

25. 1. Incompleto

26. 2. Pendiente del pedido

27 3. Pendiente de aprobación ENX

28 4. Pendiente de pago

29 5. Registrado

30 6. Activo

31 7. Expirado

Podrá encontrar las definiciones de los estados y qué ha de hacer para avanzar hasta el siguiente estado en el anexo.

Para más información sobre:

- el estado del participante, consulte la Sección 7.4, “Anexo: Participant status (Estado del participante)”.
- el estado del alcance de la evaluación, consulte la Sección 7.5, “Anexo: Assessment scope status (Estado del alcance de la evaluación)”.

4.5.10. Cambios en su información de registro

Recuerde:

Para las cuestiones relacionadas con el ciclo de vida de los datos, consulte la Sección 7.9, “Anexo: Gestión del ciclo de vida de los datos del participante”. Contiene instrucciones para aquellos casos en los que quiera cambiar o actualizar datos como el nombre de la empresa o la información de contacto.

Felicidades, ya es un participante de TISAX registrado. Está listo para continuar con el siguiente paso del proceso TISAX.

5. Evaluación (paso 2)

El tiempo de lectura estimado de la sección de evaluación es de 30-35 minutos.

5.1. Sinopsis

La evaluación TISAX es el segundo paso. Aquí es donde realiza la mayor parte del trabajo para obtener su evaluación TISAX.

Las siguientes secciones le guiarán a través de la evaluación:

1. Empezaremos explicando cómo puede usar la autoevaluación ISA para comprobar si está preparado para una evaluación TISAX.
2. A continuación, le recomendaremos cómo elegir uno de nuestros proveedores de auditoría TISAX.
3. Más adelante, describiremos su recorrido a lo largo del proceso de evaluación.
4. Por último, explicaremos el “resultado del proceso”: el resultado de la evaluación y las correspondientes etiquetas TISAX.

5.2. Autoevaluación basada en la ISA

Para estar listo para una evaluación TISAX, en primer lugar necesita tener el sistema de gestión de la seguridad de la información (ISMS) a punto. Para averiguar si su ISMS tiene el nivel de madurez esperado, ha de llevar a cabo una autoevaluación basada en la ISA.

La “evaluación de la seguridad de la información” (ISA, por sus siglas en inglés) es un catálogo de criterios publicado por la Asociación alemana de la industria automotriz (Verband der Automobilindustrie e.V., VDA). Es el estándar del sector del automóvil para las evaluaciones de la seguridad de la información.

Las siguientes secciones proporcionan instrucciones prácticas para llevar a cabo una autoevaluación basada en la ISA.

Las explicaciones, los ejemplos y las capturas de pantalla de este manual se basan en la Versión 5 de la ISA.

Recuerde:

Encontrará información sobre los cambios respecto a versiones anteriores de la ISA en la hoja de Excel “Change history” (Historial de cambios).

Recuerde:

> Para más información sobre la versión de la ISA aplicable a su evaluación cuando la VDA publique una nueva versión, consulte la Sección 7.11, “Anexo: Gestión del ciclo de vida ISA”.

5.2.1. Descarga del documento ISA

Empiece su autoevaluación descargando el documento ISA.

Puede descargarlo de nuestro sitio web en:
enx.com/en-US/TISAX/downloads/

Descarga directa del archivo Excel:
portal.enx.com/isa5-en.xlsx

El documento ISA también está disponible en alemán:
enx.com/de-de/TISAX/downloads/

5.2.2. Entender el documento ISA

Antes de empezar la autoevaluación, le damos algunas explicaciones que podrían resultarle útiles. Son adicionales a las explicaciones y definiciones oficiales del documento ISA y hacen hincapié en el uso para las evaluaciones TISAX.

5.2.2.1. Catálogos de criterios

La ISA cuenta actualmente con tres “catálogos de criterios”[13]:

1.	Seguridad de la información	Information Security
2.	Protección de prototipos	Prototype Protection
3.	Protección de datos	Data Protection

Cada catálogo de criterios tiene su propia hoja de Excel:

Figura 10. Captura de pantalla: catálogos de criterios ISA como hojas de Excel

¿Qué catálogo de criterios es relevante para usted? Esto depende de su(s) objetivo(s) de evaluación.

Cada objetivo de evaluación determina qué requisitos de cada catálogo de criterios aplicar. Para algunos objetivos de evaluación, solo se aplican los requisitos de *un* catálogo de criterios; para otros, se aplican los requisitos de *más de un* catálogo de criterios.

Los objetivos de evaluación indicados anteriormente se corresponden con estos catálogos de criterios:

Núm.	Objetivo de evaluación (Assessment objective)	Catálogo(s) de criterios ISA
1.	Info high	Information Security (Seguridad de la información)
2.	Info very high	Information Security (Seguridad de la información)
3.	Confidential	Information Security (Seguridad de la información)
4.	Strictly confidential	Information Security (Seguridad de la información)
5.	High availability	Information Security (Seguridad de la información)
6.	Very high availability	Information Security (Seguridad de la información)
7.	Proto parts	Prototype Protection (Protección de prototipos)
8.	Proto vehicles	Prototype Protection (Protección de prototipos)
9.	Test vehicles	Prototype Protection (Protección de prototipos)
10.	Proto events	Prototype Protection (Protección de prototipos)
11.	Data	Information Security (Seguridad de la información) Data Protection (Protección de datos)
12.	Special data	Information Security (Seguridad de la información) Data Protection (Protección de datos)

Tabla 7. Correspondencia entre los objetivos de evaluación TISAX y los catálogos de criterios ISA

Ejemplo: Si ha seleccionado el objetivo de evaluación “Protección de datos”, tendrá que contestar a las preguntas de los catálogos de criterios “Seguridad de la información” Y “Protección de datos”.

Habrá notado que hay más de un objetivo de evaluación para cada catálogo de criterios. ¿Cómo saber qué requisitos son aplicables a cada objetivo de evaluación?

La siguiente tabla le muestra qué requisitos son aplicables:

Núm.	Objetivo de evaluación (Assessment objective)	Requisitos aplicables
1.	Info high	▪ Catálogos de criterios “Information Security” (“Seguridad de la información”) ◦ Columna “Requirements (must)” (“Requisitos (obligatorios)”) ◦ Columna “Requirements (should)” (“Requisitos (optativos)”) ◦ Columna “Additional requirements for high protection needs” (“Requisitos adicionales para necesidad de protección alta”)
2.	Info very high	▪ Catálogos de criterios “Information Security” (“Seguridad de la información”) ◦ Columna “Requirements (must)” (“Requisitos (obligatorios)”) ◦ Columna “Requirements (should)” (“Requisitos (optativos)”) ◦ Columna “Additional requirements for high protection needs” (“Requisitos adicionales para necesidad de protección alta”) ◦ Columna ( )“Requisitos adicionales para necesidad de protección muy alta”
3.	Confidential	▪ Catálogos de criterios “Information Security” (“Seguridad de la información”) ◦ Columna “Requirements (must)” (“Requisitos (obligatorios)”) ◦ Columna “Requirements (should)” (“Requisitos (optativos)”) ◦ Columna “Additional requirements for high protection needs” (“Requisitos adicionales para necesidad de protección alta”) (pero solo los marcados con “**C**” de **C**onfidentiality (**C**onfidencialidad))

Núm.	Objetivo de evaluación (Assessment objective)	Requisitos aplicables
4.	Strictly confidential	▪ Catálogos de criterios “Information Security” (“Seguridad de la información”) ◦ Columna “Requirements (must)” (“Requisitos (obligatorios)”) ◦ Columna “Requirements (should)” (“Requisitos (optativos)”) ◦ Columna “Additional requirements for high protection needs” (“Requisitos adicionales para necesidad de protección alta”) (pero solo los marcados con “**C**” de **C**onfidentiality (**C**onfidencialidad)) ◦ Columna ( )“Requisitos adicionales para necesidad de protección muy alta” (pero solo los marcados con “**C**” de **C**onfidentiality (**C**onfidencialidad))
5.	High availability	▪ Catálogos de criterios “Information Security” (“Seguridad de la información”) ◦ Columna “Requirements (must)” (“Requisitos (obligatorios)”) ◦ Columna “Requirements (should)” (“Requisitos (optativos)”) ◦ Columna “Additional requirements for high protection needs” (“Requisitos adicionales para necesidad de protección alta”) (pero solo los marcados con “**A**” de **A**vailability (Disponibilidad))

Núm.	Objetivo de evaluación (Assessment objective)	Requisitos aplicables
6.	Very high availability	▪ Catálogos de criterios “Information Security” (“Seguridad de la información”) ◦ Columna “Requirements (must)” (“Requisitos (obligatorios)”) ◦ Columna “Requirements (should)” (“Requisitos (optativos)”) ◦ Columna “Additional requirements for high protection needs” (“Requisitos adicionales para necesidad de protección alta”) (pero solo los marcados con “**A**” de **A**vailability (Disponibilidad)) ◦ Columna ( )“Requisitos adicionales para necesidad de protección muy alta” (pero solo los marcados con “**A**” de **A**vailability (Disponibilidad))
7.	Proto parts	▪ Catálogo de criterios “Prototype Protection” (“Protección de prototipos”) Pero solo estos capítulos: 8.1 Physical and Environmental Security (8.1 Seguridad física y del entorno) 8.2 Organizational Requirements (8.2 Requisitos organizativos) 8.3 Handling of vehicles, components and parts (8.3 Manejo de vehículos, componentes y piezas) ◦ Columna “Requirements (must)” (“Requisitos (obligatorios)”) ◦ Columna “Requirements (should)” (“Requisitos (optativos)”)

Núm.	Objetivo de evaluación (Assessment objective)	Requisitos aplicables
8.	Proto vehicles	▪ Catálogo de criterios “Prototype Protection” (“Protección de prototipos”) Pero solo estos capítulos: 8.1 Physical and Environmental Security (8.1 Seguridad física y del entorno) 8.2 Organizational Requirements (8.2 Requisitos organizativos) 8.3 Handling of vehicles, components and parts (8.3 Manejo de vehículos, componentes y piezas) ◦ Columna “Requirements (must)” (“Requisitos (obligatorios)”) ◦ Columna “Requirements (should)” (“Requisitos (optativos)”) ◦ Columna “Additional requirements for vehicles classified as requiring protection” (“Requisitos adicionales para vehículos que requieren protección”)
9.	Test vehicles	▪ Catálogo de criterios “Prototype Protection” (“Protección de prototipos”) Pero solo estos capítulos: 8.2 Organizational Requirements (8.2 Requisitos organizativos) 8.3 Handling of vehicles, components and parts (8.3 Manejo de vehículos, componentes y piezas) 8.4 Requirements for trial vehicles (8.4 Requisitos para vehículos de prueba) ◦ Columna “Requirements (must)” (“Requisitos (obligatorios)”) ◦ Columna “Requirements (should)” (“Requisitos (optativos)”)

Núm.	Objetivo de evaluación (Assessment objective)	Requisitos aplicables
10.	Proto events	▪ Catálogo de criterios “Prototype Protection” (“Protección de prototipos”) Pero solo estos capítulos: 8.2 Organizational Requirements (8.2 Requisitos organizativos) 8.3 Handling of vehicles, components and parts (8.3 Manejo de vehículos, componentes y piezas) 8.5 Requirements for events and shootings (8.5 Requisitos para eventos y rodajes) ◦ Columna “Requirements (must)” (“Requisitos (obligatorios)”) ◦ Columna “Requirements (should)” (“Requisitos (optativos)”)
11.	Data	▪ Catálogos de criterios “Information Security” (“Seguridad de la información”) ◦ Columna “Requirements (must)” (“Requisitos (obligatorios)”) ◦ Columna “Requirements (should)” (“Requisitos (optativos)”) ◦ Columna “Additional requirements for high protection needs” (“Requisitos adicionales para necesidad de protección alta”) (pero solo los marcados con “**C**” de **C**onfidentiality (**C**onfidencialidad)) ▪ Catálogo de criterios “Data Protection” (“Protección de datos”) ◦ Columna “Requirements (must)” (“Requisitos (obligatorios)”)

Núm.	Objetivo de evaluación (Assessment objective)	Requisitos aplicables
12.	Special data	▪ Catálogos de criterios “Information Security” (“Seguridad de la información”) ◦ Columna “Requirements (must)” (“Requisitos (obligatorios)”) ◦ Columna “Requirements (should)” (“Requisitos (optativos)”) ◦ Columna “Additional requirements for high protection needs” (“Requisitos adicionales para necesidad de protección alta”) (pero solo los marcados con “**C**” de **C**onfidentiality (**C**onfidencialidad)) ◦ Columna ( )“Requisitos adicionales para necesidad de protección muy alta” (pero solo los marcados con “**C**” de **C**onfidentiality (**C**onfidencialidad)) ▪ Catálogo de criterios “Data Protection” (“Protección de datos”) ◦ Columna “Requirements (must)” (“Requisitos (obligatorios)”)

Tabla 8. Aplicabilidad de los requisitos a los objetivos de evaluación

Recuerde:

Cada requisito de las dos columnas “Requisitos adicionales para necesidad de protección alta” y “Requisitos adicionales para necesidad de protección muy alta” está marcado con una “**C**” de **C**onfidentiality (**C**onfidencialidad) o una “**I**” de **I**ntegrity (**I**ntegridad) o una “**A**” de **A**vailability (Disponibilidad) o cualquier combinación de estas tres letras.

Cuando la tabla anterior reduce los requisitos de estas dos columnas a los marcados con *una* de las letras mencionadas, esto incluye siempre los requisitos que también están marcados con *más* de una letra.

Ejemplo: Todos los requisitos marcados con “(C)”, “(C, I, A)” o “(C, I)” se aplican cuando se especifica “C” en la tabla superior (por ejemplo, en el objetivo de evaluación “Special data”).

La captura de pantalla que aparece a continuación muestra los principales elementos de las preguntas de control en el catálogo de criterios “Seguridad de la información”. (Los demás

catálogos de criterios solo tienen un subconjunto de estos elementos.) Explicaremos todos los elementos más adelante.

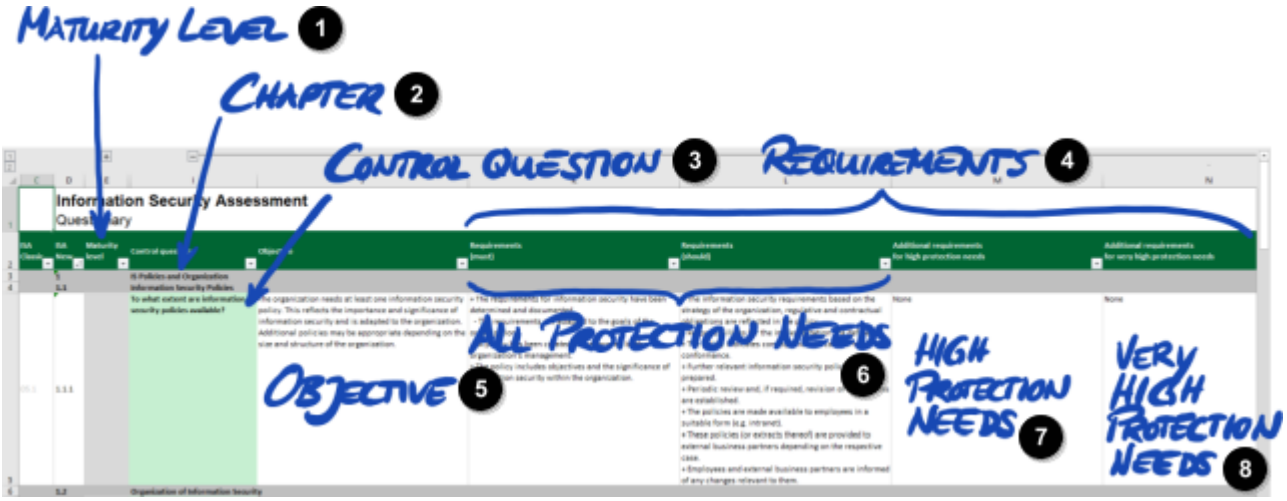


Figura 11. Captura de pantalla: Elementos principales de las preguntas en el catálogo de criterios ISA "Seguridad de la información"

1. Nivel de madurez
2. Capítulo
3. Pregunta de control
4. Requisitos
5. Objetivo
6. Todas las necesidades de protección
7. Necesidad de protección alta
8. Necesidad de protección muy alta

5.2.2.2. Capítulos

Cada catálogo de criterios agrupa las preguntas en capítulos.

Ejemplo: "2 Recursos humanos"

La agrupación se basa en las responsabilidades típicas en una empresa. Estos departamentos se especifican en la columna "Responsable habitual de la aplicación del proceso" ("RR. HH." en el ejemplo anterior).

5.2.2.3. Preguntas de control

Encontrará las preguntas para cada catálogo de criterios en las correspondientes hojas de Excel.

Ejemplo: "4.1.2 ¿Hasta qué nivel está protegido el acceso de usuarios a los servicios de red,

sistemas informáticos y aplicaciones informáticas?”

Las preguntas de control también se denominan “controles”. Esto es “jerga de auditor”. Las normas ISO en las que se basa la ISA utilizan el término “control”.

5.2.2.4. Campos del formulario de autoevaluación

Entre las columnas “Maturity level” (“Nivel de madurez”) y “Control question” (“Pregunta de control”) hay campos que deberá completar al llevar a cabo la autoevaluación:

Campo del formulario	Finalidad	¿Obligatorio?
Implementation description (Descripción de la implementación) (Columna F)	Aquí deberá describir brevemente qué ha implementado en su empresa para dar respuesta a esta pregunta de control.	Sí
Reference Documentation (Referencia a la documentación) (Columna G)	Aquí deberá especificar qué documento(s) prueba(n) esa implementación.	Sí
Findings/Result (Hallazgos/Resultado) (Columna H)	Aquí puede anotar aquellos hallazgos en los que crea que existe una brecha entre la situación real y la situación ideal.	No

Tabla 9. Campos del formulario de autoevaluación y su finalidad

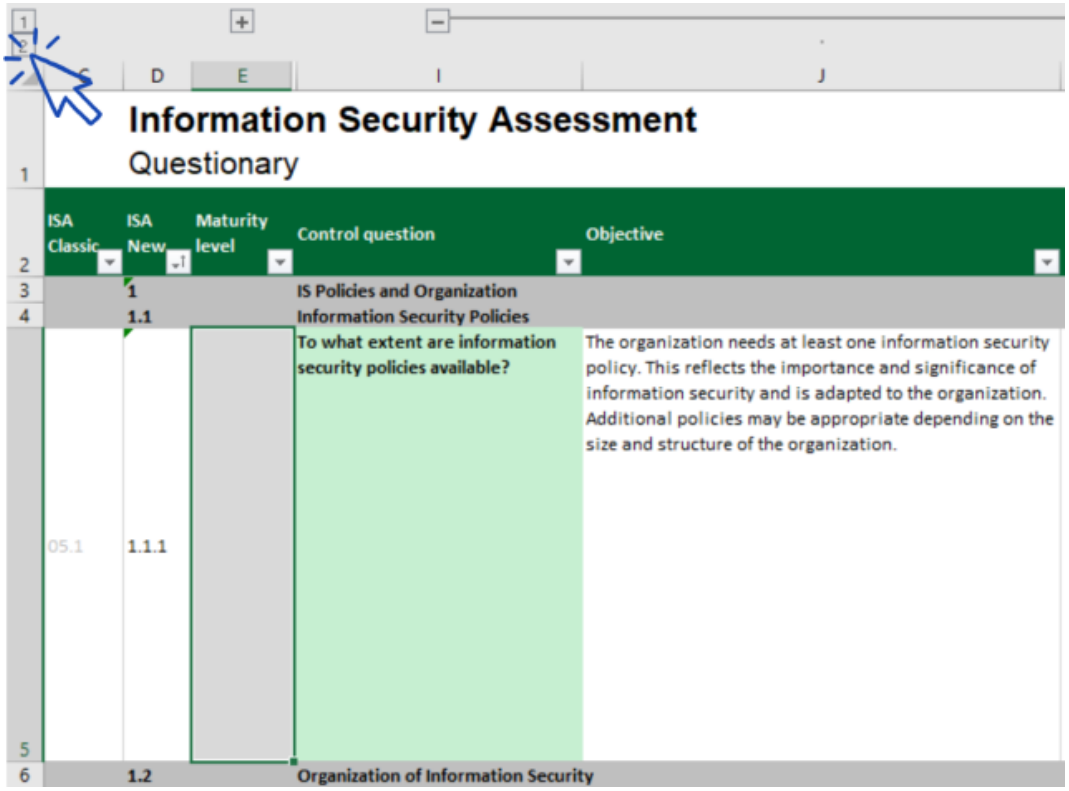
Solo son obligatorias la descripción breve de la implementación y la referencia a la documentación. Esta información ayudará a nuestros proveedores de auditoría TISAX a entender mejor su empresa y preparar la evaluación.

Hay más columnas opcionales como ayuda a su autoevaluación:

- Measures/recommendations (Medidas/Recomendaciones) (columna R)
- Date of assessment (Fecha de evaluación) (columna S)
- Date of completion (Fecha de finalización) (columna T)
- Responsible department (Departamento responsable) (columna U)
- Contact (Contacto) (columna V)

Nota importante:

Si abre el archivo de Excel descargado y selecciona una de las hojas de trabajo del catálogo de criterios (p. ej., Seguridad de la información), es probable que no vea de inmediato los campos del formulario de autoevaluación. Para mostrarlos, tendrá que hacer clic en el botón de agrupamiento para el nivel "2"[14]. El botón se encuentra por encima y a la izquierda de la celda C1. Esto expandirá la vista para mostrar los campos del formulario de autoevaluación.



Otro consejo es usar las teclas de flecha para desplazarse. Debido al tamaño de las celdas, desplazarse con la barra de desplazamiento exige excelentes habilidades de motricidad fina. Si utiliza la función de desplazamiento del dispositivo señalador, podría saltarse accidentalmente alguna de las celdas.

5.2.2.5. Objetivo

A la derecha de la columna "Pregunta de control" se encuentra la columna "Objetivo" (columna J). Su contenido describe qué debe alcanzar en ese aspecto de su gestión de la seguridad de la información.

Ejemplo (para la pregunta de control 4.1.2): "Solo los usuarios identificados de forma segura (autenticados) pueden tener acceso a los sistemas informáticos. Para este fin, la identidad de un usuario se determina de forma segura con procedimientos adecuados".

5.2.2.6. Requisitos

Los requisitos que debería cumplir para alcanzar este objetivo.

Los requisitos se reparten en cuatro columnas:

1. Requirements (must) (Requisitos (obligatorios)) (columna K)
2. Requirements (should) (Requisitos (optativos)) (columna L)
3. Additional requirements for high protection needs (Requisitos adicionales para necesidad de protección alta) (columna M)
4. Additional requirements for very high protection needs (Requisitos adicionales para necesidad de protección muy alta) (columna N)

Debe cumplir todos los requisitos hasta la necesidad de protección que debe alcanzar (que podrá deducir a partir de su objetivo de evaluación).

Para algunos objetivos de evaluación, solo se aplica un subconjunto de requisitos. Para más información sobre la aplicabilidad de los requisitos, consulte la Tabla 8, “Aplicabilidad de los requisitos a los objetivos de evaluación” en la Sección 5.2.2.1, “Catálogos de criterios” y, especialmente, la note al final de la sección.

Para más información sobre las definiciones ISA de los niveles de requisito “obligatorio” y “opcional”, consulte los “términos clave” en la hoja de Excel “Definiciones”.

Nota importante:

Es muy importante que comprenda que debe interpretar cada requisito en el contexto y el espíritu del objetivo. Incluso cumplir un requisito al pie de la letra no garantiza que el proveedor de auditoría confirme que usted lo cumple en el contexto y el espíritu del objetivo (columna J).

Los requisitos y las descripciones se basan en una implementación teórica por parte de una empresa ficticia normal de tamaño desconocido.

El proveedor de auditoría siempre debe sopesar el objetivo respecto a la implementación única en su empresa. Algo que sea adecuado para una empresa promedio podría no ser suficiente en su situación particular.

Para más información, consulte la Sección 5.2.5, “Examine el resultado de la autoevaluación”.

5.2.2.7. Niveles de madurez

La ISA utiliza el concepto de “maturity levels” (“niveles de madurez”) para puntuar la calidad de todos los aspectos de su sistema de gestión de la seguridad de la información. Cuanto más

sofisticado sea su sistema de gestión de la seguridad de la información, mayor será el nivel de madurez.

La ISA distingue seis niveles de madurez. Podrá encontrar la definición detallada en la hoja de Excel “Maturity levels” (“Niveles de madurez”). Para una visión conjunta de los niveles de madurez, citamos a continuación las descripciones informales que se recogen en la ISA:

Maturity level (Nivel de madurez)	**En una palabra**	**Descripción**
0	Incomplete (Incompleto)	No existe ningún proceso o el proceso no logra los objetivos porque no se sigue o no es adecuado.
1	Performed (Realizado)	Se sigue un proceso no documentado o documentado de forma incompleta y existen indicadores de que se han logrado los objetivos.
2	Managed (Controlado)	Se sigue un proceso que alcanza los objetivos. Se dispone de documentación del proceso y de la evidencia de la implementación del proceso.
3	Established (Establecido)	Se sigue un proceso estándar integrado en el sistema global. Las dependencias de otros procesos están documentadas y se han creado las interfaces necesarias. Existe evidencia de que el proceso se ha utilizado de forma sostenible y activa durante un periodo extenso.
4	Predictable (Predecible)	Se sigue un proceso establecido. La efectividad del proceso se controla de forma continua recopilando cifras clave. Se han definido valores límite a partir de los cuales se considera que el proceso no es lo suficientemente efectivo y requiere ajustes. (Indicadores clave de rendimiento)
5	Optimizing (Optimizando)	Se sigue un proceso predecible con la mejora continua como objetivo principal. La mejora se impulsa activamente mediante recursos específicos.

Tabla 10. Descripción informal de los niveles de madurez

Ha de valorar el nivel de madurez de su sistema de gestión de la seguridad de la información para cada pregunta. Introduzca su nivel de madurez en la columna “Maturity level” (“Nivel de madurez”) (columna E).

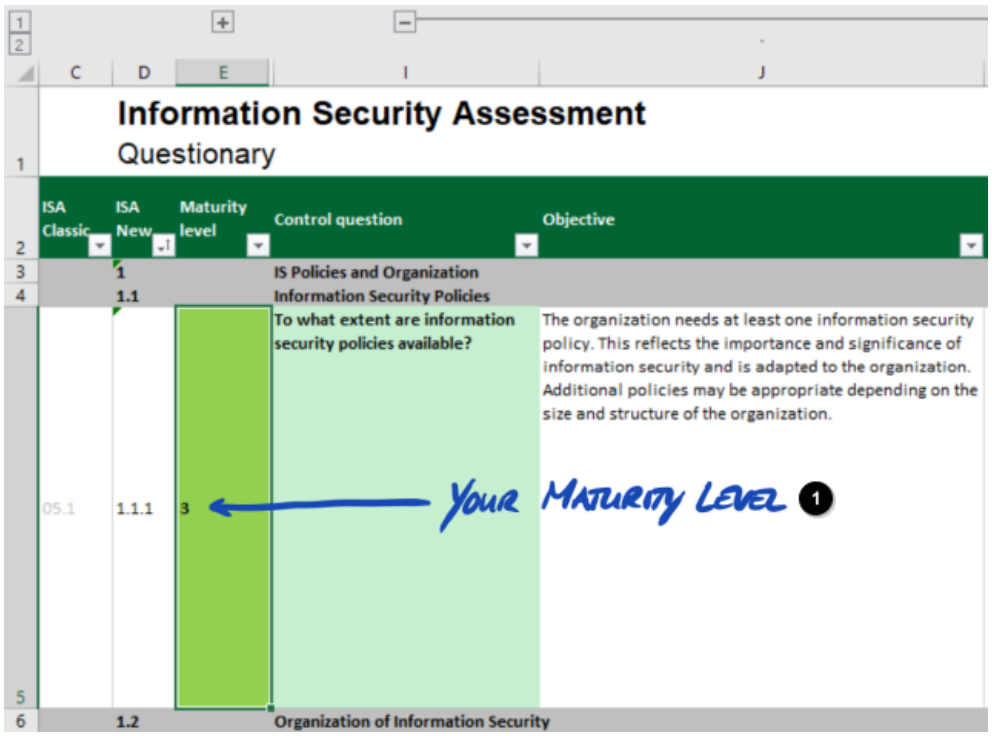


Figura 12. Captura de pantalla: Ejemplo de selección del nivel de madurez en el documento ISA (hoja de Excel "Seguridad de la información")

1 Su nivel de madurez

Para más información sobre los niveles de madurez objetivo y su impacto en el resultado de la evaluación, consulte la Sección 5.2.4, "Interpretar el resultado de la autoevaluación".

Con estos conocimientos, ahora está listo para iniciar la autoevaluación.

5.2.3. Realizar la autoevaluación

Abra el archivo de Excel y responda a todas las preguntas de control de cada catálogo de criterios aplicable a su(s) objetivo(s) de evaluación y determine el nivel de madurez que corresponda al estado actual de su sistema de gestión de la seguridad de la información. Responda según su entender. No hay respuestas correctas y equivocadas en esta fase.

Una vez completada la autoevaluación, la columna "Resultado" (H) de la hoja de Excel "Resultados (ISA5)" debería estar completamente cumplimentada, con números (0-5) o con "n.a." ("no aplicable").

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3
1.2.3	To what extent are information security requirements taken into account in projects?	3	3
1.2.4	To what extent are responsibilities between external IT service providers and the own organization defined?	3	3
1.3.1	To what extent are information assets identified and recorded?	3	3
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	3	3
1.3.3	To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?	3	3
1.4.1	To what extent are information security risks managed?	3	3
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	3	3
1.5.2	To what extent is the ISMS reviewed by an independent entity?	3	3
1.6.1	To what extent are information security events processed?	3	3

❶ GREEN = ✓

Figura 13. Captura de pantalla: Ejemplo de la hoja "Resultados (ISA5)" del documento ISA

❶ Verde

Si tiene preguntas sobre la ISA, póngase en contacto con nosotros.

5.2.4. Interpretar el resultado de la autoevaluación

Las siguientes cinco subsecciones explican cómo analizar e interpretar el resultado de la autoevaluación. El análisis le dirá si está listo o no para una evaluación TISAX.

5.2.4.1. Análisis

La puntuación final resume el resultado de la autoevaluación.

Encontrará la puntuación final ("Resultado con reducción a los niveles de madurez objetivo") en la hoja de Excel "Resultados (ISA5)" (celda D6). Explicaremos la "reducción" pronto.

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

Details: YOUR RESULT SCORE 1 MAXIMUM RESULT SCORE 2

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Figura 14. Captura de pantalla: Su puntuación final y el resultado máximo (hoja de Excel "Resultados (ISA5)", celda D6 y G6).

1. Su puntuación final
2. Resultado máximo

Para entender e interpretar el resultado de la autoevaluación y su puntuación final, debe diferenciar dos niveles de análisis:

1. Nivel de pregunta
   Este nivel tiene todas las preguntas. Para cada pregunta, hay un nivel de madurez objetivo y su nivel de madurez.
2. Nivel de puntuación
   En este nivel, hay un resultado total que resume los resultados de todas las preguntas. Existe un resultado máximo y su puntuación final.

La figura inferior muestra los niveles de análisis:

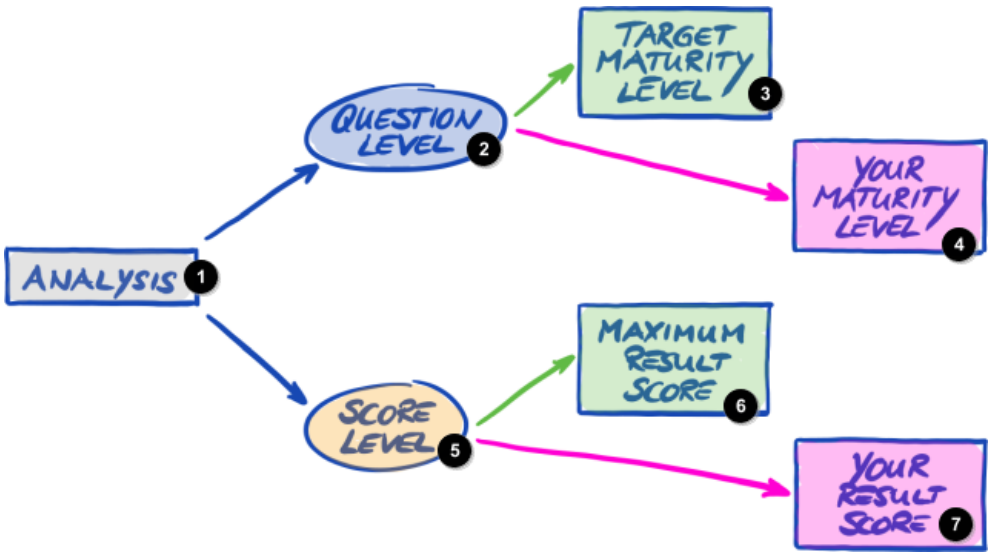


Figura 15. Análisis del resultado de la autoevaluación a nivel de pregunta y nivel de puntuación

1. Análisis
2. Nivel de pregunta
3. Nivel de madurez objetivo
4. Su nivel de madurez
5. Nivel de puntuación
6. Resultado máximo
7. Su puntuación final

La figura inferior muestra dónde encontrará los resultados a nivel de puntuación y los resultados a nivel de pregunta:

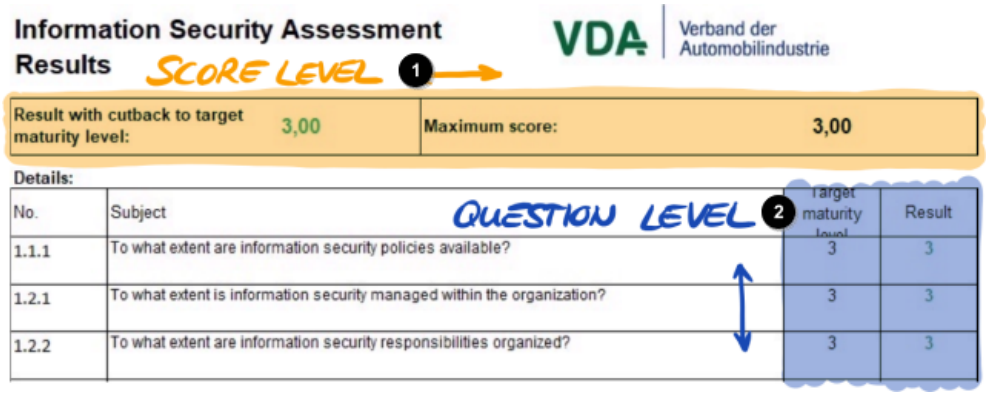


Figura 16. Nivel de puntuación y nivel de pregunta en la hoja de Excel "Resultados (ISA5)"

1. Nivel de puntuación
2. Nivel de pregunta

La siguiente figura muestra una vista simplificada de los niveles de análisis, las definiciones de objetivos de la ISA y sus propios resultados:

Figura 17. Los objetivos y sus resultados a nivel de pregunta y nivel de puntuación

1. Nivel de madurez objetivo
2. Su nivel de madurez
3. Nivel de pregunta
4. Q (Pregunta)
5. TML (Nivel de madurez objetivo)
6. YML (Su nivel de madurez)
7. Resultado máximo
8. Su puntuación final
9. Nivel de puntuación

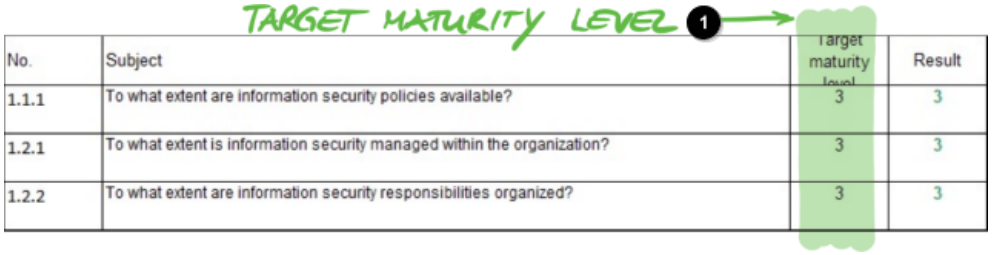
Las siguientes secciones explican el resultado y su análisis en detalle.

5.2.4.2. El nivel de madurez objetivo (a nivel de pregunta)

La ISA define un “nivel de madurez objetivo” de 3 para cada pregunta.

Para más información sobre la definición de cada nivel de madurez, consulte la Sección 5.2.2, “Entender el documento ISA”.

La ISA define los niveles de madurez objetivo en la hoja de Excel “Resultados (ISA5)” (empezando por la columna G, fila 22, vea la figura más abajo).



No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Figura 18. La definición de nivel de madurez objetivo en la hoja de Excel “Resultados (ISA5)”

1. Nivel de madurez objetivo

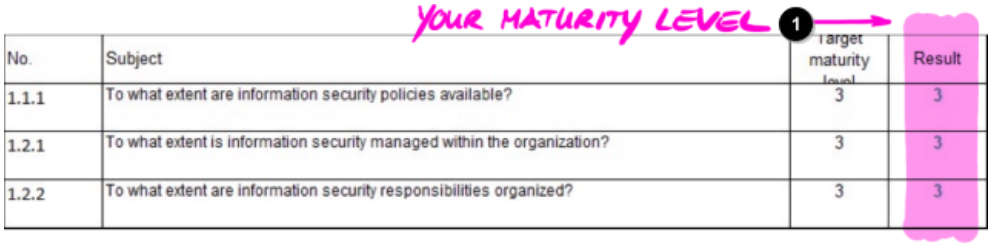
5.2.4.3. Su resultado (a nivel de pregunta)

Para recibir etiquetas TISAX, normalmente debe tener para cada pregunta un nivel de madurez igual o superior al nivel de madurez objetivo.

Ejemplo: Si el nivel de madurez objetivo para la pregunta X es “3”, su nivel de madurez para esa pregunta debería ser “3” o superior. Si su nivel de madurez para la pregunta está por debajo de “3”, podría no recibir etiquetas TISAX.

Esto ha de ser así para cada pregunta. Si el nivel de madurez objetivo de dos preguntas es “3”, no puede compensar un nivel de madurez “2” en una pregunta con un nivel de madurez “4” en otra pregunta.

El documento ISA automáticamente transfiere los niveles de madurez de la hoja de Excel “Seguridad de la información” (columna E) a la hoja de Excel “Resultados (ISA5)” (empezando por la columna H, fila 23):



No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Figura 19. Sus niveles de madurez en la hoja de Excel “Resultados (ISA5)”

1. Su nivel de madurez objetivo

Su nivel de madurez se somete a un cálculo antes de que el documento ISA lo resuma en la puntuación final. Básicamente, su nivel de madurez se "reduce" al nivel de madurez objetivo. Esto se hace así de forma que las preguntas en las que su nivel de madurez está *por encima* del nivel de madurez objetivo no compensen las preguntas en las que el nivel de madurez está *por debajo* del nivel de madurez objetivo.

Así calcula la ISA su resultado a nivel de pregunta:

- Toma su nivel de madurez y lo compara con el nivel de madurez objetivo de la pregunta.
- Si su nivel de madurez es superior al nivel de madurez objetivo, lo "reduce" al nivel de madurez objetivo.
- Si su nivel de madurez es igual o inferior al nivel de madurez objetivo, no se hace nada a la pregunta.

Ejemplo (vea la figura más abajo): El nivel de madurez objetivo es "3". Su nivel de madurez es "4". Su "resultado reducido" para esa pregunta será "3".

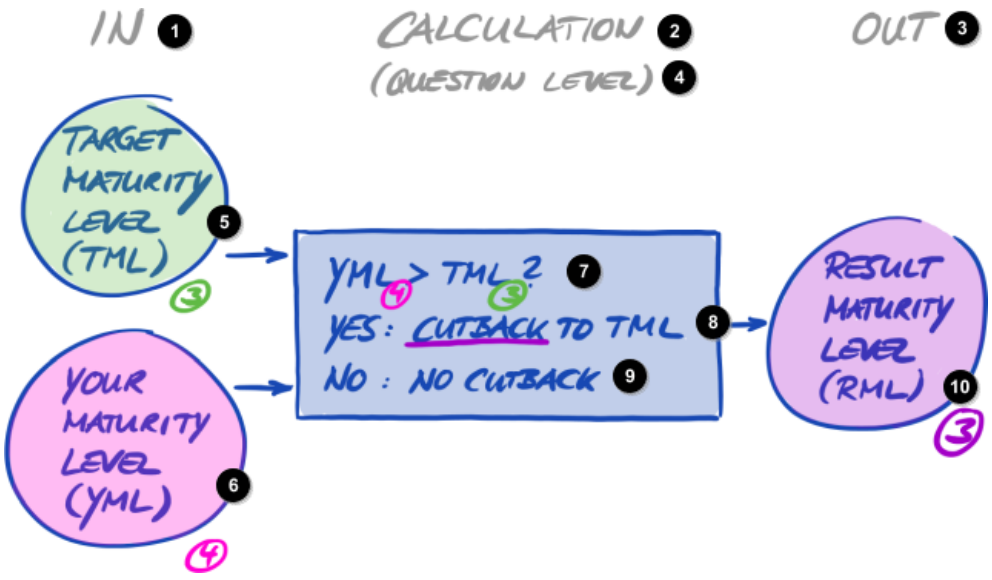


Figura 20. Reducción del nivel de madurez resultante

1. Entrada
2. Cálculo
3. Salida
4. (Nivel de pregunta)
5. Nivel de madurez objetivo (TML)
6. Su nivel de madurez (YML)

7. ¿YML > TML?
8. Sí: reducción a TML
9. No: sin reducción
10. Nivel de madurez resultante (RML)

La siguiente figura muestra que, si su nivel de madurez es superior al nivel de madurez objetivo, la ISA lo reduce (los colores verde, naranja y rojo coinciden con los colores usados en la columna “Resultado”, véase la Figura 19, “Sus niveles de madurez en la hoja de Excel “Resultados (ISA5)””).

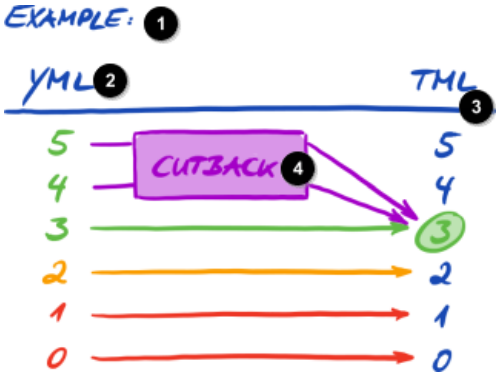


Figura 21. Ilustración de la reducción con los colores usados en la hoja de Excel “Resultados (ISA5)”

1. Ejemplo:
2. YML
3. TML
4. Reducción

A continuación se muestra otra forma de ver los niveles de madurez a nivel de pregunta. Los colores de los círculos ilustran el nivel de madurez objetivo o la “distancia” hasta dicho nivel (ejemplo: el círculo es naranja si el nivel de madurez está “-1” por debajo del nivel de madurez objetivo). Las marcas de verificación ilustran su nivel de madurez.

Figura 22. Niveles de madurez a nivel de pregunta

1. Nivel de madurez
2. Pregunta
3. Reducción
4. Nivel de madurez objetivo (TML)
5. Uno o más por encima del TML
6. Uno por debajo del TML
7. Dos o más por debajo del TML
8. Su nivel de madurez (YML)
9. Reducción al TML

Recuerde:

Es posible superar la evaluación TISAX incluso si no alcanza el nivel de madurez objetivo para todas las preguntas. En ese caso, la principal pregunta será si tiene un riesgo relevante. Si su nivel de madurez está por debajo del valor objetivo pero no existe ningún riesgo, podría ser suficiente.

5.2.4.4. El objetivo (a nivel de puntuación)

La ISA define un nivel de madurez global “ideal”: el “resultado máximo” (o “Puntuación máxima”, celda G6).

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

MAXIMUM RESULT SCORE

Details:

No.	Subject	Target maturity level	Result ❶
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Figura 23. Resultado máximo (hoja de Excel “Resultados (ISA5)”)

❶ Resultado máximo

En teoría, el nivel de madurez global es la media de todos los niveles de madurez objetivo (a nivel de pregunta). Esto daría un resultado máximo de “3,0”.

Sin embargo, solo es “3,0” si todas las preguntas son aplicables a su situación. En cuanto una pregunta no es aplicable a su situación, el promedio cambia y el resultado máximo será inferior a “3,0”.

A partir de la vista mostrada (Figura 22, “Niveles de madurez a nivel de pregunta”), a continuación verá qué se incluye en el promedio para el resultado máximo:

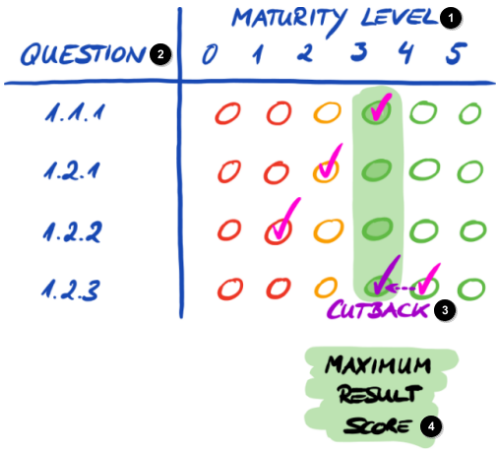


Figura 24. El resultado máximo (a nivel de puntuación)

❶ Nivel de madurez

❷ Pregunta

❸ Reducción

❹ Resultado máximo

5.2.4.5. Su resultado (a nivel de puntuación)

Su puntuación final total (“Resultado con reducción a los niveles de madurez objetivo”, celda D6):

- resume el nivel de madurez total de su sistema de gestión de la seguridad de la información.
- es la media de sus niveles de madurez (a nivel de pregunta).
- puede ser igual o inferior al resultado máximo.
- debería estar lo más cerca posible del resultado máximo. Cuanto más lejos esté su puntuación final del resultado máximo, menos probable es que reciba etiquetas TISAX.

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

Details: YOUR RESULT SCORE ❶

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

Figura 25. Su puntuación final (hoja de Excel “Resultados (ISA5)”)

❶ Su puntuación final

De nuevo a partir de la vista mostrada (Figura 22, “Niveles de madurez a nivel de pregunta”), a continuación verá qué se incluye en el promedio para la puntuación final:

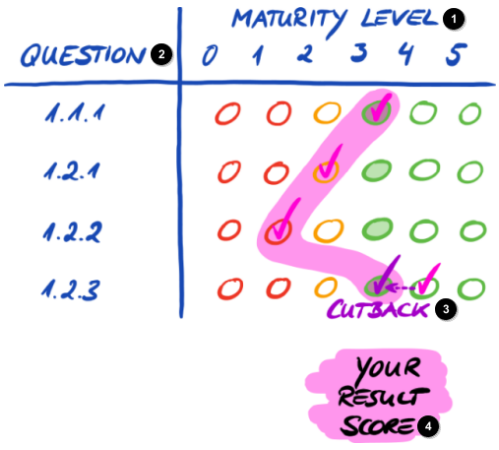


Figura 26. Su puntuación final (a nivel de puntuación)

❶ Nivel de madurez

❷ Pregunta

3. Reducción
4. Su puntuación final

La puntuación final le dice si:

- está listo para una evaluación TISAX.
- puede esperar recibir etiquetas TISAX.

Si su puntuación final (“Resultado con reducción a los niveles de madurez objetivo”) está por debajo de “3,0”, significa que al menos en una pregunta su nivel de madurez no coincide con el nivel de madurez objetivo. En ese caso, es probable que tenga que mejorar su sistema de gestión de la seguridad de la información antes de estar listo para su evaluación TISAX.

Recuerde:

Para la puntuación total, existen límites formales para una “distancia” aceptable entre su puntuación final y el resultado máximo (“Resultado con reducción a los niveles de madurez objetivo”).

Si su puntuación final se encuentra más:

- del 10 % por debajo, el resultado global de la evaluación será “no conforme con una desviación mínima”.
- del 30 % por debajo, el resultado global de la evaluación será “no conforme con una desviación importante”.

Nota importante:

Tener una puntuación final (“Resultado con reducción a los niveles de madurez objetivo”) de “3” no es garantía de que superará la evaluación TISAX sin hallazgos negativos. Tenga en cuenta que el proveedor de auditoría puede ver ciertos aspectos de forma diferente a usted.

5.2.4.6. ¿Está listo?

El objetivo del análisis anterior es saber si está listo para una evaluación TISAX.

Estará listo para una evaluación TISAX si su puntuación final (“Resultado con reducción a los niveles de madurez objetivo”) es de “3,0” (o cercano a ese valor). En ese caso, todos los valores de la columna “Resultados” (H) estarán en verde (no en naranja o rojo).

Si no están en verde, deberá seguir analizando el resultado de la autoevaluación (consulte la Sección 5.2.5, “Examine el resultado de la autoevaluación”).

La siguiente figura muestra un diagrama de telaraña ISA de la hoja de Excel “Resultados (ISA5)”. La línea verde marca el nivel de madurez objetivo por cada capítulo. Si sus niveles de madurez están en esa línea o por encima, está listo para una evaluación TISAX. Si están por debajo de esa línea, podría no ser suficiente para obtener etiquetas TISAX.

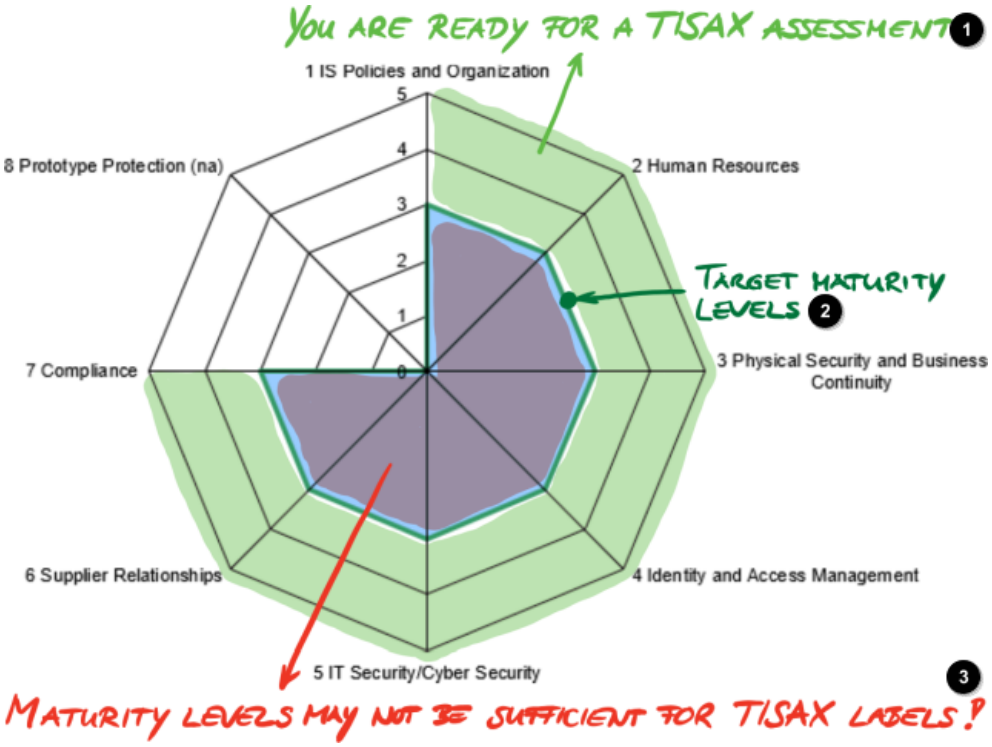


Figura 27. Captura de pantalla: Cumplimiento del nivel de madurez objetivo en el diagrama de telaraña ISA (hoja de Excel “Resultados (ISA5)”)

1. Está listo para la evaluación TISAX
2. Niveles de madurez objetivo
3. ¡Los niveles de madurez pueden no bastar para obtener etiquetas TISAX!

Si “despliega” la telaraña ISA al nivel de pregunta, obtendrá una imagen verde/roja similar a nivel de pregunta:

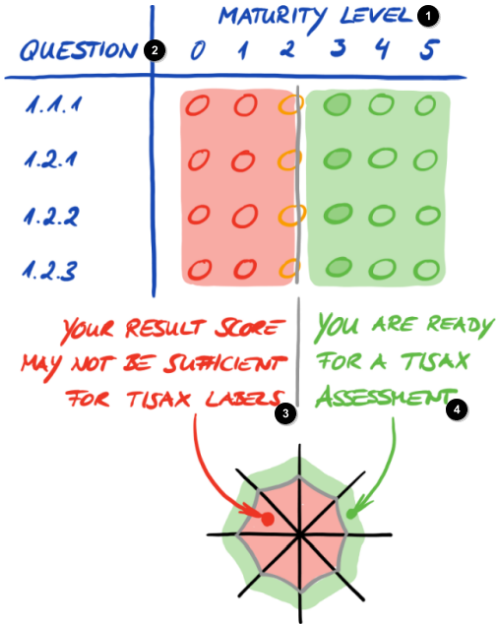


Figura 28. "Despliegue" del diagrama de telaraña ISA

1. Nivel de madurez
2. Pregunta
3. Su puntuación final puede no bastar para obtener etiquetas TISAX
4. Está listo para la evaluación TISAX

5.2.5. Examine el resultado de la autoevaluación

El resultado de su autoevaluación podría mostrar que necesita mejorar su sistema de gestión de la seguridad de la información antes de poder recibir las etiquetas TISAX.

Es posible que ya sepa cómo cerrar algunas brechas entre su nivel de madurez y el nivel de madurez objetivo. Para otras, puede que necesite asesoramiento externo. En ese caso, puede solicitar servicios de consultoría a nuestros proveedores de auditoría TISAX. TISAX permite que actúen como consultores, pero no lo exige. Recuerde que un proveedor de auditoría que le preste servicios de consultoría ya no podrá encargarse de su evaluación TISAX.

Nota importante:

No analizar correctamente el resultado de la autoevaluación *antes* de la evaluación supone un gran escollo para muchas empresas. No subestime los esfuerzos necesarios para adaptar su sistema de gestión de la seguridad de la información a los requisitos. Muchas empresas necesitan iniciar un proyecto de envergadura para prepararse para una evaluación TISAX.

Recuerde:

Si busca ayuda externa para llevar a cabo el proceso TISAX, verá que existen muchas empresas que ofrecen servicios de consultoría y formación. Ninguna de esas empresas están asociadas con nosotros.

A día de hoy:

- no ofrecemos cursos de formación oficiales, ni directamente ni a través de terceros.
- no valoramos la calidad de los servicios de terceros, por lo que aconsejamos precaución.

Recuerde:

No recomendamos solicitar partidas como “pre-evaluación” o “análisis de deficiencias”. Si bien entendemos el deseo de prepararse para la evaluación de esa forma, en la mayoría de los casos es más útil empezar la evaluación directamente.

Para más información sobre por qué no recomendamos una pre-evaluación, consulte la Sección 7.7, “Anexo: El razonamiento en contra de las “pre-evaluaciones” y los “análisis de deficiencias””.

5.3. Selección del proveedor de auditoría

Solo los proveedores de auditoría autorizados por nosotros pueden llevar a cabo evaluaciones TISAX[15]. Los proveedores de auditoría TISAX solo están autorizados a llevar a cabo sus evaluaciones TISAX si previamente no le han prestado servicios de consultoría.

Todos nuestros proveedores de auditoría TISAX están obligados a llevar a cabo evaluaciones TISAX únicamente a empresas que son participantes registrados de TISAX.

Nota importante:

En cuanto haya registrado un alcance de la evaluación TISAX, *deberá* empezar a ponerse en contacto con nuestros proveedores de auditoría. Tienen ciertos tiempos de espera en lo que respecta a su disponibilidad. Ponerse en contacto con ellos *después* de terminar los preparativos podría suponer un retraso innecesario.

Recuerde:

Cada alcance de la evaluación tiene un ciclo de vida. Llegados a este punto, su alcance de la evaluación debe tener el estado “Approved” (Aprobado) o

> “Registered” (Registrado)
>
> Para más información sobre el estado de un alcance de la evaluación, consulte la Sección 7.5.5, “Assessment scope status “Awaiting your payment” (Estado del alcance de la evaluación “Pendiente de pago”)”.

5.3.1. Información de contacto

Una vez que haya registrado un alcance de la evaluación TISAX, podrá ponerse en contacto con todos los proveedores de auditoría TISAX y solicitar ofertas. La información de contacto figura en el mensaje de confirmación del registro que ha recibido[16] (consulte la Sección 4.5.8, “Mensaje de correo electrónico de confirmación”).

> Recuerde:
>
> Solicite ofertas a nuestros proveedores de auditoría TISAX solo DESPUÉS de haberse registrado. Los proveedores de auditoría comprobarán si está registrado. Sin registro, han de rechazar las peticiones.
>
> Este es el motivo por el que recibe la información de contacto de los proveedores de auditoría en el mensaje de confirmación del registro y no en nuestro sitio web público.

5.3.2. Cobertura

Aunque actualmente un gran número de los proveedores de auditoría están en Alemania, recuerde que todos nuestros proveedores de auditoría son capaces de llevar a cabo evaluaciones TISAX en todo el mundo. La mayoría tiene incluso empleados propios en muchos países.

En nuestro sitio web, ofrecemos una página en la que puede seleccionar su país y ver qué proveedor de auditoría tiene personal de ventas local y/o auditores locales (enx.com/en-US/TISAX/xap/).

5.3.3. Solicitud de ofertas

Para que nuestros proveedores de auditoría TISAX puedan calcular correctamente los esfuerzos de evaluación esperados, siempre deberá incluir el “TISAX Scope Excerpt”.

Figura 29. Miniatura de un “TISAX Scope Excerpt” (primera página)

Para más información, consulte la Sección 4.5.8, “Mensaje de correo electrónico de confirmación”.

Recuerde:

La imparcialidad es una característica clave de nuestros proveedores de auditoría TISAX. Ellos se asegurarán de que no haya conflictos de intereses. Téngalo en cuenta cuando se ponga en contacto con ellos. Si su empresa tiene algún tipo de relación con un proveedor de auditoría, no espere que se encargue de su evaluación.

5.3.4. Valoración de las ofertas

Puede elegir libremente entre todos nuestros proveedores de auditoría TISAX. Todos están sujetos al mismo contrato. Todos llevan a cabo evaluaciones basadas en los mismos criterios y los mismos métodos de auditoría. En términos del resultado de la evaluación, no habrá diferencias independientemente del proveedor de auditoría que elija. El resultado de su evaluación será aceptado por todos los participantes de TISAX.

Aparte de factores obvios como precio, reputación y simpatía, hay algunos aspectos de las ofertas en los que se puede fijar:

- Disponibilidad:
  ¿Cuándo puede empezar el proceso de evaluación? Este puede ser un aspecto importante si obtener su evaluación TISAX es urgente.
- Costes de viajes para sesiones in situ:
  Los proveedores de auditoría con oficinas en su país probablemente tendrán costes de viajes más bajos.
- Idioma:
  ¿Usted y el resto de personas entrevistadas de su empresa podrán comunicarse con el auditor en su idioma nativo?
- Alcance de la oferta:

¿Qué evaluaciones están incluidas?
Para más información sobre las evaluaciones, consulte la Sección 5.4.3, “Tipos de evaluación TISAX”.
Normalmente, las ofertas incluyen la evaluación inicial y la evaluación del plan de acciones correctivas. Como resulta difícil predecir el esfuerzo de las evaluaciones de seguimiento, este servicio se suele ofrecer una vez finalizadas las otras evaluaciones.

Al final, todo se reduce a la confianza. Ha de forjar una relación de confianza con su proveedor de auditoría, puesto que tendrá una visión bastante exhaustiva de su empresa.

Recuerde:

No recomendamos solicitar partidas como “pre-evaluación” o “análisis de deficiencias”. Si bien entendemos el deseo de prepararse para la evaluación de esa forma, en la mayoría de los casos es más útil empezar la evaluación directamente.

Para más información sobre por qué no recomendamos una pre-evaluación, consulte la Sección 7.7, “Anexo: El razonamiento en contra de las “pre-evaluaciones” y los “análisis de deficiencias””.

Recuerde:

Aunque nos gustaría poder decirle cuánto cobrarán nuestros proveedores de auditoría por la evaluación, entienda que es una información que no podemos proporcionar. Los costes dependen de demasiados factores. Además, nuestros proveedores de auditoría son libres a la hora de realizar sus cálculos comerciales.

No obstante, podemos mencionar algunas estimaciones bastante aproximadas sobre el número de jornadas que le cobrarán nuestros proveedores de auditoría. Para una pequeña empresa promedia con una sola ubicación, deberá contar con entre tres jornadas y media y cuatro jornadas para una evaluación en el nivel de evaluación 2 y entre cinco y seis jornadas para una evaluación en el nivel de evaluación 3.

Recuerde:

Cada evaluación tiene un ciclo de vida.

Para más información sobre el estado de una evaluación, consulte la Sección 7.6, “Anexo: Assessment status (Estado de la evaluación)”.

Una vez que haya escogido a uno de nuestros proveedores de auditoría TISAX, podrá finalmente

iniciar el proceso de evaluación TISAX.

5.4. Proceso de evaluación TISAX

5.4.1. Sinopsis

El proceso de evaluación TISAX consiste en varios tipos de evaluación. En la mayoría de los casos habrá más de una evaluación.

Deberá ver el proceso de evaluación como una secuencia interconectada de pasos en la que:

- Usted prepara su sistema de gestión de la seguridad de la información para que esté en plena forma.
- El proveedor de auditoría comprueba si su sistema de gestión de la seguridad de la información cumple un conjunto determinado de requisitos. El auditor puede encontrar brechas.
- Usted cierra esas brechas en un periodo definido.
- El proveedor de auditoría comprueba de nuevo si se han cerrado las brechas.

Estos pasos se repiten hasta que todas las brechas se han cerrado.

Es importante entender que *usted* inicia cada paso intermedio en el proceso de evaluación. Todo el proceso de evaluación está bajo su control. Y, lógicamente, usted puede decidir parar y finalizar el proceso de evaluación en cualquier momento.[17]

El proceso de evaluación TISAX tiene la siguiente macroestructura:

- Reunión inicial
  Usted y el proveedor de auditoría planifican los detalles del proceso de evaluación
- Fase de evaluación 1
  El proveedor de auditoría comprueba la autoevaluación
- Fase de evaluación 2
  El proveedor de auditoría lleva a cabo la o las evaluaciones

5.4.2. Reunión inicial

El proceso de evaluación TISAX comienza con la reunión inicial. Aquí se planifican los detalles del proceso de evaluación. Normalmente, la reunión inicial se realiza por teleconferencia. El proveedor de auditoría le guiará a lo largo de la reunión.

En el orden del día figuran, entre otros, los siguientes temas:

- ¿Quiénes son los participantes de la reunión?

- ¿Quién es la empresa evaluada?
- ¿Cómo funciona el proceso de evaluación TISAX?
- ¿Cuál es el alcance de la evaluación y es correcto?
- ¿Existen conflictos de intereses?
- ¿Cómo es una buena autoevaluación?
- ¿Quién es responsable de qué?
- ¿Cómo nos vamos a comunicar?
- ¿Cuándo se llevará a cabo la evaluación (y otra planificación temporal)?
- ¿Quién debe participar en la o las evaluaciones?
- ¿A quién puede dirigirse si tiene una reclamación?

El periodo de tiempo entre el final de la reunión inicial y la entrega de la autoevaluación suele ser de uno a tres meses. Pero un plazo de seis meses tampoco es inusual. Depende del estado de preparación. TISAX no impone plazos para este periodo. Puede tomarse todo el tiempo que necesite para preparar la autoevaluación y para prepararse para la evaluación.

5.4.3. Tipos de evaluación TISAX

El proceso de evaluación TISAX consta de estos tres tipos de evaluación TISAX:

- Evaluación inicial (Initial assessment)
- Evaluación del plan de acciones correctivas (Corrective action plan assessment)
- Evaluación de seguimiento (Follow-up assessment) [18]

La evaluación inicial siempre se llevará a cabo. Las otras dos evaluaciones TISAX pueden o no darse y pueden darse más de una vez. Se llevarán a cabo:

- hasta que cierre todas las brechas
- o hasta que abandone el proceso de evaluación TISAX
- o bien hasta que alcance el periodo máximo de nueve meses desde la finalización de la reunión final de la evaluación inicial (en ese momento, se requerirá otra evaluación inicial).

Todas las evaluaciones TISAX se describen en las secciones siguientes.

Recuerde:

Cada evaluación tiene un ciclo de vida.

Para más información sobre el estado de una evaluación, consulte la Sección 7.6, “Anexo: Assessment status (Estado de la evaluación)”.

5.4.4. Elementos de la evaluación TISAX

Cada evaluación TISAX consta de los siguientes elementos:

- Reunión inicial formal[19][20]
  - Pretende cubrir todos los temas organizativos.
  - No tiene por qué ser una reunión presencial.
  - Los temas se pueden tratar en una sesión o bien repartirse a lo largo de varias sesiones.
  - Es un “contenedor lógico” para todos los temas organizativos *previos* a la evaluación.
- Procedimiento de evaluación
  - Su proveedor de auditoría comprobará todos los requisitos.
  - Se seleccionarán los métodos de evaluación de acuerdo con el nivel de evaluación en cuestión.
- Reunión final formal[21]
  - Cierra la evaluación TISAX.
  - El proveedor de auditoría presenta sus hallazgos.
  - El proveedor de auditoría anuncia el resultado de la evaluación.
  - No tiene por qué ser una reunión presencial.
  - Es un “contenedor lógico” para todos los temas organizativos *posteriores* a la evaluación.

Después de la “reunión final”, el proveedor de auditoría prepara y le envía el borrador del “informe de evaluación TISAX” actualizado. Usted puede expresar sus objeciones si opina que el proveedor de auditoría ha malinterpretado algo.[22] A continuación, el proveedor de auditoría emite el “informe de evaluación TISAX” definitivo.

Todos estos elementos se describirán en las próximas secciones.

5.4.5. Acerca de la conformidad

Antes de continuar con el proceso de evaluación TISAX, queremos explicar un concepto clave esencial para que entienda las siguientes secciones.

El objetivo de una evaluación TISAX es determinar si su sistema de gestión de la seguridad de la información cumple un conjunto determinado de requisitos. El proveedor de auditoría comprueba si su sistema de gestión de la seguridad de la información es “conforme” (“conforms”) con los requisitos.

Paso 1: Se comprueba cada requisito aplicable individualmente.

Si su enfoque es “conforme” con todos los requisitos, usted supera la evaluación y recibe las

etiquetas TISAX correspondientes a sus objetivos de evaluación.

Todo aquello que esté por debajo de la conformidad plena o ideal se denominará “hallazgo” (🇬🇧 finding). TISAX distingue entre cuatro tipos de hallazgo:

Núm.	Tipo	Definición	Reacción	Ejemplos
1.	No conformidad *mayor* (🇬🇧 *Major* non-conformity)	Una no conformidad *mayor*: ▪ supone un riesgo inmediato considerable para la seguridad de su información ▪ **o** genera dudas sobre la eficacia general de su sistema de gestión de la seguridad de la información	Debe: ▪ abordar inmediatamente una no conformidad *mayor* con medidas compensatorias adecuadas ▪ implementar medidas correctivas sin demora	▪ No conformidades sistemáticas ▪ Déficits de implementación que suponen riesgos críticos para la seguridad de la información confidencial ▪ Déficits de implementación que no se abordan mediante una acción correctiva adecuada
2.	No conformidad *menor* (🇬🇧 *Minor* non-conformity)	Una no conformidad *menor*: ▪ *no* supone un riesgo inmediato considerable para la seguridad de su información ▪ **y** *no* genera dudas sobre la eficacia general de su sistema de gestión de la seguridad de la información	Debe: ▪ implementar medidas correctivas sin demora	▪ Fallos aislados o esporádicos ▪ Incumplimiento o déficit en la implementación de los requisitos o de sus políticas

Núm.	Tipo	Definición	Reacción	Ejemplos
3.	Observación (Observation)	Una observación es un incumplimiento de los requisitos de sus propias políticas que no supone un riesgo inmediato para la seguridad de su información pero que puede suponerlo en el futuro.	Debe: ▪ investigar, controlar y evaluar cuidadosamente los posibles riesgos ▪ decidir cómo tratar la observación	n/a
4.	Margen de mejora (Room for improvement)	Una desviación que no pertenezca a los tipos anteriores y que no supone un riesgo para la seguridad de su información, pero que ofrece un margen de mejora evidente.	Usted puede decidir si aborda este tipo de hallazgo y cómo.	n/a

Tabla 11. Los cuatro tipos de hallazgo

Paso 2: Todos los resultados del paso previo “por requisito” se agrupan en un resultado global de la evaluación.

El resultado global de la evaluación puede ser:

a. Conforme (Conform)
   El resultado global de la evaluación es “conforme”. Todos los requisitos se cumplen

b. No conforme con una desviación mínima (Minor non-conform)
   El resultado global de la evaluación es “no conforme con una desviación mínima” si tiene al menos una “no conformidad menor” para uno de los requisitos.

c. No conforme con una desviación importante (Major non-conform)
   El resultado global de la evaluación es “no conforme con una desviación importante” si tiene al menos una “no conformidad mayor” para uno de los requisitos.
   (Si no se dispone de un plan de acciones correctivas aprobado, cualquier no conformidad dará un resultado global de la evaluación de “no conforme con una desviación importante”.)

Si su resultado global de la evaluación es:

- “no conforme con una desviación mínima”, podrá recibir etiquetas TISAX *temporales* hasta

que se resuelvan todas las no conformidades.

- “no conforme con una desviación importante”, ha de resolver el tema correspondiente antes de poder recibir etiquetas TISAX.
  Con medidas de compensación adecuadas y acciones correctivas aprobadas por el proveedor de auditoría, es posible cambiar el resultado global de la evaluación de “no conforme con una desviación importante” a “no conforme con una desviación mínima” y recibir las etiquetas TISAX temporales.

Es importante que entienda que el resultado global de la evaluación mejorará durante el transcurso del proceso de evaluación TISAX.

Tenga en cuenta este ejemplo simplificado: puede que tenga un resultado global de la evaluación de “no conforme con una desviación importante” después de la evaluación inicial. A continuación, mitiga el riesgo correspondiente. Esto cambiará el resultado global de la evaluación de “no conforme con una desviación importante” a “no conforme con una desviación mínima”. Y una vez que haya eliminado el riesgo, su resultado global de la evaluación final será “conforme”.

Todo esto se explicará más adelante con mucho más detalle. Y también podrá encontrar más información sobre las etiquetas TISAX en: Sección 5.4.14, “Etiquetas TISAX”.

5.4.6. Su preparación para el proceso de evaluación TISAX

El proveedor de auditoría preparará la evaluación en función de su autoevaluación. Por tanto, tenga en cuenta que deberá facilitar la autoevaluación a su proveedor de auditoría con antelación. Las fechas de entrega exactas se acuerdan durante la reunión inicial.

Un proveedor de auditoría bien preparado reducirá el tiempo necesario para la evaluación. Además de la autoevaluación, también solicitará documentación pertinente antes de la evaluación. Esta puede ser la documentación que haya citado en la autoevaluación o cualquier otra documentación que el proveedor de auditoría considere relevante.

A partir de esta información, su proveedor de auditoría planificará el procedimiento de evaluación.

5.4.7. Evaluación inicial

Esta es la primera evaluación TISAX y marca el inicio formal del proceso de evaluación TISAX.

Nota importante:

La evaluación inicial marca el inicio de dos periodos importantes:

1. El periodo máximo de validez de las etiquetas TISAX es de tres años.
2. Dispone de hasta nueve meses para resolver las no conformidades. Si no

resuelve todas las no conformidades dentro de este plazo, no recibirá etiquetas TISAX. No obstante, si se le pasa este plazo, puede continuar directamente con una nueva evaluación inicial.

Ambos periodos comienzan el día de la reunión final de la evaluación inicial.

Recuerde:

Aparte de los dos periodos descritos anteriormente, no existen otras limitaciones temporales. Por ejemplo, ni completar el proceso de registro online, ni ponerse en contacto con nuestros proveedores de auditoría, ni siquiera celebrar la reunión inicial, activan ningún plazo. Depende de usted comenzar con la evaluación inicial.

5.4.7.1. La primera reunión inicial formal

Como todas las evaluaciones TISAX, la evaluación inicial empieza con una reunión inicial formal. La reunión inicial formal suele realizarse mediante teleconferencia o videoconferencia. Para pequeñas empresas, posiblemente con alguna experiencia de otras auditorías, no lleva mucho tiempo.

El objetivo de esta reunión es:

- comprobar los requisitos previos de la evaluación
- presentar al jefe del proyecto de evaluación y al equipo de evaluación
- planificar la evaluación

5.4.7.2. Procedimiento de evaluación

Según el plan elaborado, el proveedor de auditoría llevará a cabo la evaluación inicial. Los detalles concretos dependerán de sus objetivos de evaluación. La evaluación consiste principalmente en teleconferencias, entrevistas in situ e inspecciones in situ con diferentes grados de exhaustividad[23].

El proveedor de auditoría presentará todos sus hallazgos durante la evaluación inicial.

5.4.7.3. Reunión final

En la reunión final, su proveedor de auditoría resumirá de nuevo todos sus hallazgos.

5.4.7.4. Informe de evaluación TISAX

Después de la reunión final, el proveedor de auditoría preparará y le enviará el borrador del “informe de evaluación TISAX”. Usted puede expresar sus objeciones si opina que el proveedor de auditoría ha malinterpretado algo.[24] A continuación, el proveedor de auditoría emite el

“informe de evaluación TISAX”.

En esta fase, el resultado global de la evaluación actual será:

- Conforme, o
- No conforme con una desviación importante
  Cualquier no conformidad (menor) sin abordar siempre conlleva un resultado global de la evaluación de “no conforme con una desviación importante”. Su resultado global de la evaluación solo puede ser “no conforme con una desviación mínima” una vez que haya definido acciones que implementen medidas para abordar las no conformidades.
  Para más información sobre cómo lograrlo, consulte la Sección 5.4.9.4, “Etiquetas TISAX temporales”.

Si su resultado global de la evaluación es “conforme” tras la evaluación inicial, puede saltarse el resto de la sección sobre las evaluaciones y proceder al intercambio de su resultado.

Si su resultado global de la evaluación es “no conforme con una desviación importante”, la próxima tarea será elaborar un plan para abordar los hallazgos y cerrar las brechas encontradas por el proveedor de auditoría. Este plan se llama oficialmente “plan de acciones correctivas” (“corrective action plan”).

Recuerde:

Si, antes de que comience la evaluación, sabe de una situación que dará lugar a una no conformidad y no podrá solucionarla antes de la evaluación, podría planificar ya una acción correctiva (incluida una fecha de implementación) y presentarla al proveedor de auditoría durante la evaluación. Esto, teóricamente, podría conducir a un resultado de evaluación global de "no conforme con una desviación mínima". No obstante, sería una situación *excepcional*.

5.4.8. Preparación del plan de acciones correctivas

Su “plan de acciones correctivas” (“corrective action plan”) define cómo prevé abordar los hallazgos de la evaluación inicial. Su proveedor de auditoría evaluará la adecuación de su “plan de acciones correctivas” (vea la siguiente sección).

Para crear su “plan de acciones correctivas”, debería considerar los siguientes requisitos:

- Hallazgo
  - Debe indicar qué hallazgo aborda la acción correctiva.
- Causa raíz
  - Debe identificar y describir la causa raíz del hallazgo.

- Acciones correctivas
  - Por cada no conformidad deberá definir una o más “acciones correctivas” que implementarán medidas para abordar la no conformidad.
- Fecha de implementación
  - Debe definir una fecha de implementación para cada acción correctiva.
  - El periodo de implementación debe dar tiempo suficiente para implementar las medidas a fondo.
- Medidas de compensación
  - Para todas las no conformidades que crean riesgos críticos, deberá definir medidas de compensación que aborden las no conformidades hasta que las acciones correctivas se hayan implementado.
- Periodo de implementación
  - Para todas las acciones correctivas que necesiten más de tres meses de implementación deberá justificar el periodo de implementación.
  - Para todas las acciones correctivas que necesiten más de seis meses, además deberá presentar evidencias de que una implementación más rápida no es posible.
  - El periodo de implementación para cualquier acción correctiva no puede ser superior a nueve meses.

Una vez completado el plan de acciones correctivas, podrá solicitar la “evaluación del plan de acciones correctivas”.

Nota importante:

Recomendamos que inicie la implementación lo antes posible. No hace falta esperar el resultado de la “evaluación del plan de acciones correctivas”.
La “evaluación del plan de acciones correctivas” suele llevarse a cabo una vez que ha entregado el plan de acciones correctivas a su proveedor de auditoría.

Recuerde:

TISAX solo tiene requisitos en cuanto al contenido, no en cuanto a la forma de los planes de acciones correctivas.
La mayoría de nuestros proveedores de auditoría ofrecen plantillas para los planes de acciones correctivas.

5.4.9. Evaluación del plan de acciones correctivas

La finalidad de la “evaluación del plan de acciones correctivas” es verificar que su “plan de acciones correctivas” (vea la información anterior) cumple los requisitos TISAX.

Usted envía el “plan de acciones correctivas” a su proveedor de auditoría. El proveedor de auditoría evaluará el plan según los requisitos (consulte más abajo). Si el plan cumple los requisitos, el proveedor de auditoría emitirá el “informe de evaluación TISAX” actualizado.

Esta evaluación no acostumbra a requerir mucho tiempo. En la mayoría de los casos, se tratará de una teleconferencia o videoconferencia. A veces incluso se gestiona tan solo por correo electrónico.

5.4.9.1. Motivos de una evaluación del plan de acciones correctivas

Los motivos de una “evaluación del plan de acciones correctivas” son:

- Sigue habiendo no conformidades después de
  - una evaluación inicial
  - una evaluación de seguimiento
  - una evaluación de la ampliación del alcance
- Un “plan de acciones correctivas” que ya se había evaluado pero no cumplía los requisitos
- Los factores de influencia en los que se basa el cálculo de los plazos de implementación de un plan de medidas correctivas han cambiado

5.4.9.2. Combinación con la evaluación inicial

La “evaluación del plan de acciones correctivas” no es obligatoriamente un evento independiente. Tiene la opción de presentar el “plan de acciones correctivas” durante la reunión final de la evaluación inicial. El proveedor de auditoría puede entonces llevar a cabo la “evaluación del plan de acciones correctivas” directamente.

Si combina la “evaluación del plan de acciones correctivas” con la evaluación inicial y su “plan de acciones correctivas” cumple los requisitos, podrá acordar con el proveedor de auditoría que no necesita un “informe de evaluación inicial”. En su lugar, el proveedor de auditoría simplemente prepararía el “informe de evaluación del plan de acciones correctivas”. Este informe le permite recibir etiquetas TISAX temporales.

5.4.9.3. Requisitos del plan de acciones correctivas

El proveedor de auditoría evalúa su “plan de acciones correctivas” de acuerdo con los siguientes requisitos:

- Las medidas son adecuadas
  - El proveedor de auditoría evaluará la idoneidad de una acción correctiva en función de si resolverá la causa raíz de la no conformidad.
- Los riesgos críticos se mitigan con medidas de compensación adecuadas[25]
- Los periodos de implementación son adecuados

- Los periodos de implementación empiezan el día en que se concluye la evaluación inicial

- Ningún periodo de implementación es superior a:
  - tres meses sin justificación adicional
  - seis meses sin justificación adicional y evidencias
  - nueve meses

5.4.9.4. Etiquetas TISAX temporales

Si su resultado global de la evaluación es “no conforme con una desviación mínima”, recibirá etiquetas TISAX temporales.

La ventaja de las etiquetas TISAX temporales es que su socio habitualmente las acepta bajo la condición de que más adelante usted reciba las etiquetas TISAX definitivas. Esto puede resultar útil si le urge demostrar a su socio la efectividad de su sistema de gestión de la seguridad de la información.

El requisito previo para obtener etiquetas TISAX temporales es la existencia de un informe de evaluación del plan de acciones correctivas con el resultado global de la evaluación “no conforme con una desviación mínima”.

Las etiquetas temporales TISAX equivalen a las etiquetas TISAX definitivas. La única diferencia es el periodo de validez más corto de las etiquetas temporales TISAX.

Las etiquetas temporales TISAX pueden ser válidas hasta nueve meses después de la reunión final de la evaluación inicial. El periodo de validez de las etiquetas temporales TISAX está determinado por el mayor periodo de implementación de las acciones correctivas.

Ejemplos:

- Solo tiene una no conformidad. Debe llevar a cabo una revisión de la política. El periodo de implementación asociado es de *dos* meses.
  En ese caso, sus etiquetas temporales TISAX son válidas durante *dos* meses.
- Tiene la no conformidad de la revisión de la política mencionada anteriormente. Además, tiene una no conformidad por la que tiene que construir un nuevo muro exterior como acción correctiva. Debido al tiempo que se tarda en obtener los permisos necesarios del ayuntamiento, el periodo de implementación asociado es de *ocho* meses.
  En ese caso, sus etiquetas temporales TISAX son válidas durante *ocho* meses.

Para más información sobre los requisitos de los periodos de implementación, consulte la Sección 5.4.9.3, “Requisitos del plan de acciones correctivas”

Recuerde:

La “evaluación del plan de acciones correctivas” es opcional.

> Puede ir directamente a la evaluación de seguimiento si:
>
> - no necesita etiquetas TISAX temporales y
> - confía en implementar acciones correctivas sin necesidad de que el proveedor de auditoría apruebe el plan

Una vez que haya completado todas las acciones correctivas, deberá solicitar una “evaluación de seguimiento”.

5.4.10. Evaluación de seguimiento

El objetivo de la “evaluación de seguimiento” es evaluar si se han resuelto todas las no conformidades identificadas previamente. Por lo general, usted solicitará la evaluación de seguimiento cuando esté seguro de que todas las no conformidades están resueltas.

Pero puede tener tantas evaluaciones de seguimiento como necesite. Si durante una evaluación de seguimiento el proveedor de auditoría sigue identificando no conformidades o incluso detecta nuevas, usted simplemente deberá actualizar el plan de acciones correctivas e iniciar esta parte del proceso de evaluación de nuevo.

La evaluación puede ser una reunión presencial o una teleconferencia o videoconferencia.

5.4.10.1. Calendario

Su proveedor de auditoría puede realizar la o las evaluaciones de seguimiento durante los nueve meses siguientes a concluir la evaluación inicial[26].

5.4.10.2. Requisitos previos

Si no necesita etiquetas TISAX temporales, puede solicitar directamente una evaluación de seguimiento. No necesita tener una “evaluación del plan de acciones correctivas” antes de la evaluación de seguimiento.

5.4.10.3. Vencimiento de las etiquetas TISAX temporales

En caso de que necesite etiquetas TISAX temporales, asegúrese de que no haya un lapso temporal hasta recibir las etiquetas TISAX definitivas. Por este motivo, le recomendamos que solicite la evaluación de seguimiento con mucha antelación respecto a la última fecha posible[27]. Querrá tener suficiente margen de tiempo para ocuparse de cualquier hallazgo menor identificado durante la evaluación de seguimiento.

5.4.11. Diagrama del proceso de evaluación TISAX

Las secciones anteriores se resumen en el siguiente diagrama de proceso:

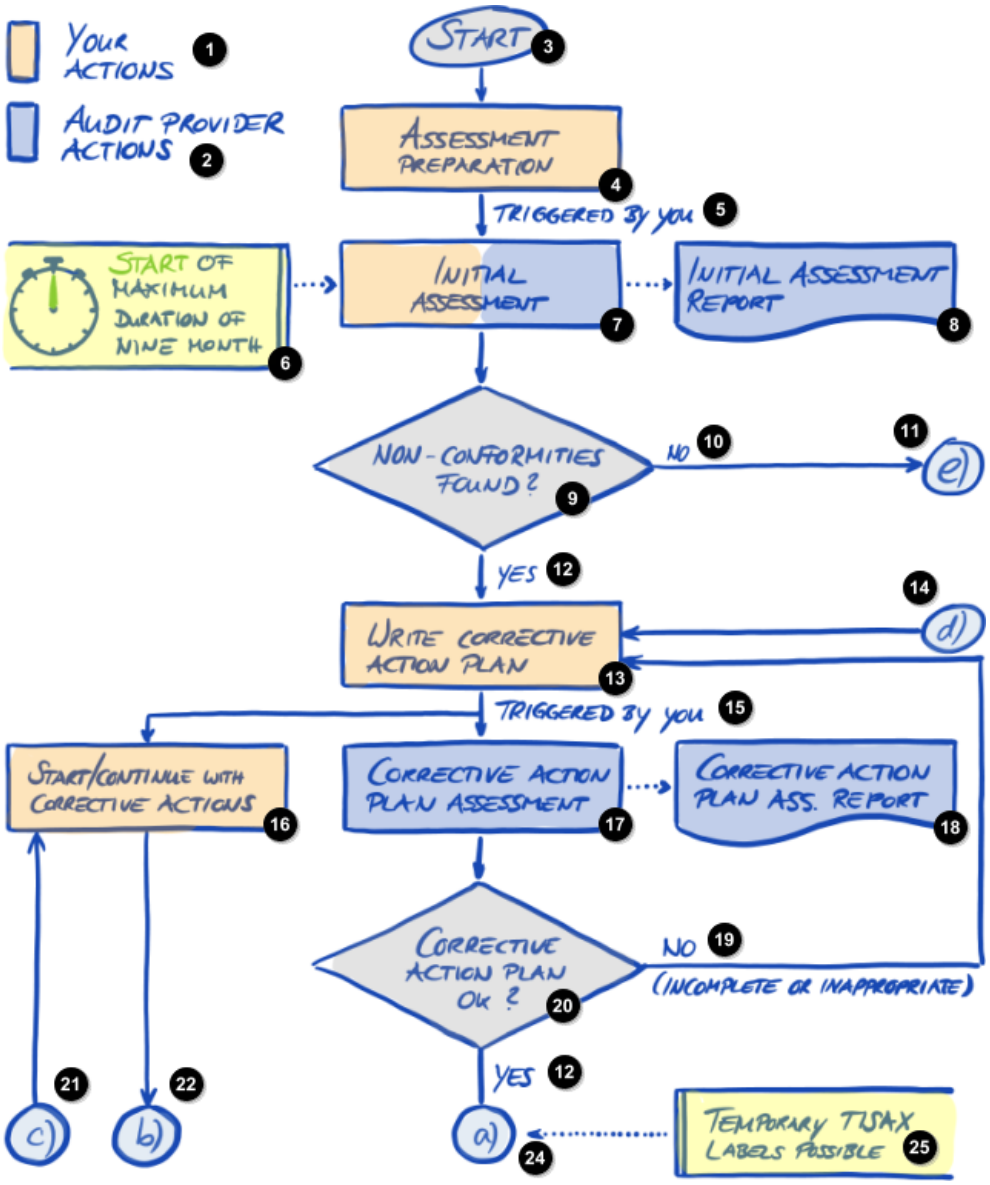


Figura 30. Diagrama del proceso de evaluación TISAX (parte 1/2)

1. Sus acciones
2. Acciones del proveedor de auditoría
3. Inicio
4. Preparación de la evaluación
5. Iniciado por usted
6. Inicio de la duración máxima de nueve meses
7. Evaluación inicial
8. Informe de evaluación inicial
9. ¿No conformidades encontradas?

10 No

11 e)

12 Sí

13 Redactar el plan de acciones correctivas

14 d)

15 Iniciado por usted

16 Iniciar/continuar con las acciones correctivas

17 Evaluación del plan de acciones correctivas

18 Informe de evaluación del plan de acciones correctivas

19 No (incompleto o inadecuado)

20 ¿Plan de acciones correctivas correcto?

21 c)

22 b)

24 a)

25 Etiquetas TISAX temporales posibles

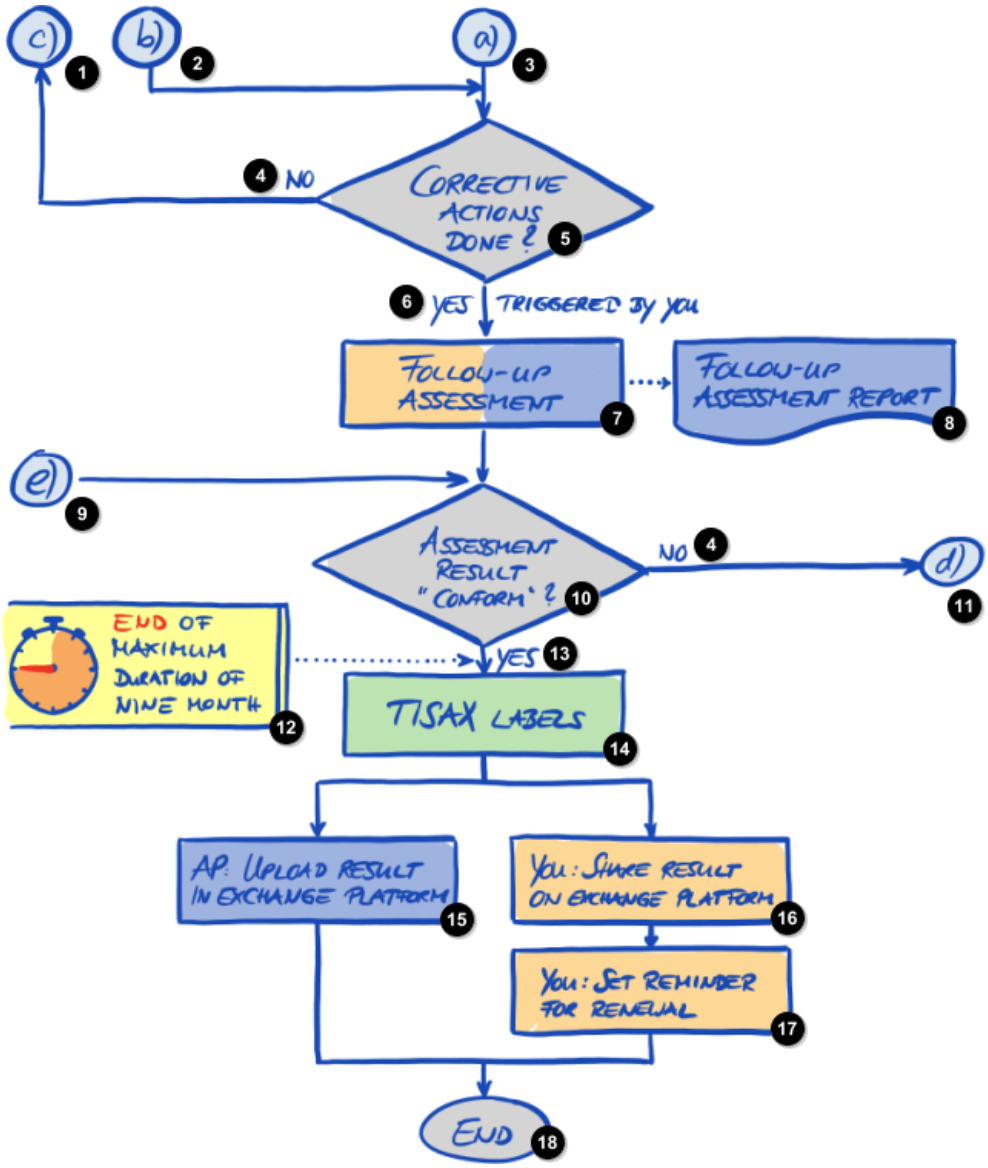


Figura 31. Diagrama del proceso de evaluación TISAX (parte 2/2)

1. c)
2. b)
3. a)
4. No
5. ¿Acciones correctivas implementadas?
6. Sí, iniciado por usted
7. Evaluación de seguimiento
8. Informe de la evaluación de seguimiento
9. e)

10. ¿Resultado de la evaluación “conforme”?
11. d)
12. Fin de la duración máxima de nueve meses
13. Sí
14. Etiquetas TISAX
15. Proveedor de auditoría: carga el resultado en la plataforma de intercambio
16. Usted: comparte el resultado en la plataforma de intercambio
17. Usted: activa el recordatorio de renovación
18. Fin

5.4.12. Assessment ID (ID de evaluación)

Cada evaluación TISAX de un alcance de la evaluación se identifica mediante un “ID de evaluación”. El ID remite a su resultado de evaluación y al correspondiente informe de evaluación TISAX.

El ID de evaluación tiene este aspecto:

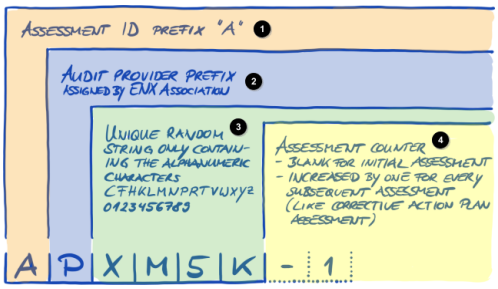


Figura 32. Formato del ID de evaluación

1. Prefijo “A” del ID de evaluación
2. Prefijo del proveedor de auditoría asignado por ENX Association
3. Secuencia aleatoria única, compuesta solo por los caracteres alfanuméricos:
   CFHKLMNPRTVWXYZ
   0123456789
4. Contador de evaluación
   - En blanco para la evaluación inicial
   - Incrementado en uno con cada evaluación sucesiva (como la evaluación del plan de acciones correctivas)

El ID de evaluación se usa normalmente cuando el proveedor de auditoría se comunica con

usted.

5.4.13. Informe de evaluación TISAX

El “informe de evaluación TISAX” (🇬🇧 “TISAX assessment report”):

- se (actualiza y) expide tras cada evaluación TISAX.
- documenta los hallazgos de su proveedor de auditoría.
- contiene el resultado global de la evaluación (conforme, no conforme con una desviación mínima, no conforme con una desviación importante).
- contiene el resto de información relacionada con su evaluación TISAX (como el objetivo de la evaluación, el alcance, las personas implicadas y las ubicaciones).

El “informe de evaluación TISAX” puede ser de los siguientes tipos (dependiendo del tipo de evaluación):

- Informe de evaluación *inicial* (🇬🇧 *Initial* assessment report)
- Informe de evaluación del *plan de acciones correctivas* (🇬🇧 *Corrective action plan* assessment report)
- Informe de evaluación de *seguimiento* (🇬🇧 *Follow-up* assessment report) [28]

El “informe de evaluación TISAX” siempre tiene la misma estructura[29]. Su proveedor de auditoría únicamente lo amplía tras cada evaluación. Esto significa que solo tendrá que tratar con la última versión del informe de evaluación TISAX, ya que siempre incluirá el contenido de las versiones anteriores.

Las primeras secciones del “informe de evaluación TISAX” son lo que finalmente comparte con su socio.

Una de las características clave de TISAX es que usted decide qué partes del informe de evaluación TISAX quiere compartir con su socio u otro participante. La estructura del informe de evaluación TISAX está diseñada para permitir esta divulgación selectiva. Cada sección incrementa el nivel de detalle.

Así es la estructura del “informe de evaluación TISAX”:

- A. Información relacionada con la evaluación
  Nombre de la empresa, alcance de la evaluación, ID de alcance, ID de evaluación, nivel de evaluación, objetivo(s) de evaluación, fecha(s) de evaluación, proveedor de auditoría
  Esta sección no contiene el resultado de la evaluación.
- B. Resultados resumidos
  Resumen de gestión del resultado de la evaluación (conforme, no conforme con una desviación mínima, no conforme con una desviación importante), número de hallazgos,

categorización abstracta de los riesgos resultantes

- C. Resumen del resultado de la evaluación
  Resumen del resultado de la evaluación por cada capítulo (por ejemplo, “9 Control de acceso”) y por cada catálogo de criterios (por ejemplo, “Seguridad de la información”).
- D. Niveles de madurez de VDA ISA (pestaña de resultados)
  Nivel de madurez para cada requisito
- E. Resultados detallados de la evaluación
  Descripción detallada de todos los hallazgos, resultados de la evaluación de riesgos, medidas necesarias, periodo de implementación

En el paso “intercambio” (detallado más abajo), usted decide hasta qué nivel tendrá acceso su socio respecto al contenido del informe de evaluación TISAX.

5.4.14. Etiquetas TISAX

Hemos tratado brevemente este tema en la sección dedicada a los preparativos para el registro. Como habíamos explicado, los objetivos de la evaluación se convierten en etiquetas TISAX.

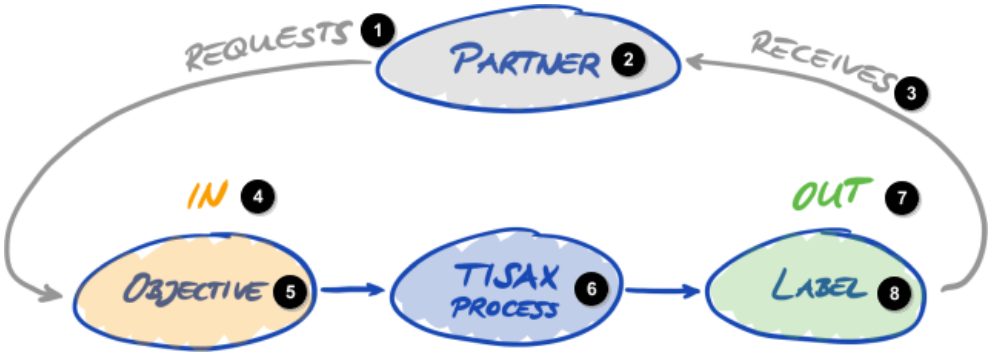


Figura 33. Objetivos de evaluación y etiquetas TISAX

1. Solicita
2. Socio
3. Recibe
4. ENTRADA
5. Objetivo
6. Proceso TISAX
7. SALIDA
8. Etiqueta

Las etiquetas TISAX:

- son el producto del proceso de evaluación TISAX.
- resumen el resultado de la evaluación.
- son la confirmación de que su sistema de gestión de la seguridad de la información cumple un conjunto determinado de requisitos.

El uso de etiquetas TISAX facilita la comunicación relativa a TISAX con su socio y con el proveedor de auditoría TISAX porque remite a un resultado definido del proceso de evaluación TISAX.

5.4.14.1. Jerarquía de las etiquetas TISAX

La correspondencia entre los objetivos de evaluación y las respectivas etiquetas TISAX es bastante clara. Pero también hay un aspecto importante: *algunas* etiquetas TISAX tienen relaciones jerárquicas. Esto significa que, si recibe una determinada etiqueta TISAX, automáticamente recibirá las etiquetas TISAX "por debajo" de esa etiqueta.

Ejemplo: Si su objetivo de evaluación era "Very high availability", recibirá la correspondiente etiqueta TISAX "Very high availability". Pero como el objetivo de evaluación "Very high availability" es un superconjunto de "High availability", recibirá automáticamente también la etiqueta TISAX "High availability".

Esta jerarquía existe actualmente para estas etiquetas TISAX:

- "Info high" es un superconjunto de "Confidential" y "High availability".
- "Info very high" es un superconjunto de "Strictly confidential" y "Very high availability".
- "Strictly confidential" es un superconjunto de "Confidential".
- "Very high availability" es un superconjunto de "High availability".
- "Special data" es un superconjunto de "Data".

Recuerde:

También puede recibir etiquetas TISAX con carácter retroactivo. Cuando introducimos una nueva etiqueta que es un subconjunto de una de las etiquetas TISAX que ya ha recibido, recibe automáticamente la nueva etiqueta.

Ejemplo: Usted recibió la etiqueta TISAX "Info high" en un momento en el que la etiqueta "High availability" aún no existía. Cuando introdujimos la etiqueta High availability, nuestro sistema se la asignó automáticamente.

Puede obtener estas relaciones jerárquicas comparando los requisitos aplicables especificados en la Tabla 8, "Aplicabilidad de los requisitos a los objetivos de evaluación".

Esta cuestión puede no ser importante para algunos participantes. Pero imagine que un socio le

solicita que le muestre la etiqueta TISAX “Very high availability” y otro le pide la etiqueta TISAX “High availability”. En ese caso, tener ambas etiquetas TISAX se lo pone fácil a todos, ya que así nadie tiene que entender que “High availability” es un subconjunto de “Very high availability”. Este caso puede darse especialmente en socios para los que disponer de ciertas etiquetas TISAX forma parte de un proceso de compra bastante rígido. Seguramente preferirá no tener que explicar que “Very high availability” es “mejor” que “High availability”. Bastará con que le muestre todas sus etiquetas TISAX a la persona que le evalúa y esta podrá marcar el requisito “Debe tener la etiqueta TISAX 'High availability'”.

5.4.14.2. Periodo de validez de las etiquetas TISAX

Las etiquetas TISAX suelen ser válidas durante tres años. El periodo de validez empieza al final del proceso de evaluación (incluso antes de que se emita el informe de evaluación TISAX).

El periodo de validez puede incluso ser menor si se han producido cambios importantes en el alcance de la evaluación TISAX.

Ejemplos: reubicación de su empresa, nuevas ubicaciones. (Para recibir instrucciones sobre qué hacer en esos casos, consulte la Sección 7.9.3.2, “Cómo solicitar un cambio de ubicación” y la Sección 7.9.3.4, “Cómo añadir una ubicación adicional”.)

Recuerde:

Solo puede ver sus etiquetas TISAX en el portal ENX. No están registradas en el informe de evaluación TISAX.

5.4.14.3. Renovación de las etiquetas TISAX

Para mantener sus etiquetas TISAX a largo plazo, deberá renovarlas[30] cada tres años.

Para ello, básicamente debe pasar el proceso TISAX de nuevo (registrar un alcance de la evaluación, obtener de nuevo la evaluación TISAX y compartir el resultado de la evaluación). El registro es algo más fácil porque no tendrá que volver a crear su empresa como participante de TISAX. Y, lógicamente, puede reusar todos los contactos y ubicaciones guardados en la base de datos TISAX.

Nota importante:

Registre un NUEVO alcance ANTES de dirigirse a su proveedor de auditoría. Su proveedor de auditoría solo puede iniciar un nuevo proceso de evaluación si puede facilitarle un nuevo ID de alcance.

En la mayoría de los casos, registrar un nuevo alcance es fácil. Solo tiene que asignar un nuevo nombre de alcance, añadir contactos, seleccionar el o los objetivos de evaluación y añadir ubicaciones. Puede reusar los contactos y las

ubicaciones que ya están en el sistema de un alcance registrado con anterioridad.

Nota importante:

Vuelva a utilizar los registros de ubicación existentes que creó y utilizó durante el registro de su alcance anterior. No cree un nuevo registro de ubicación con la misma dirección.

Motivo: Algunos participantes de TISAX procesan los resultados de evaluación de sus socios automáticamente. A tal fin, sincronizan su propio sistema con el portal ENX. Incluso las diferencias más insignificantes pueden provocar un fallo de sincronización. Además, no debería recargar sus datos de participante con duplicados innecesarios.

Nota importante:

Si su socio le requiere que siempre tenga etiquetas TISAX válidas durante su relación, le recomendamos encarecidamente que fije un recordatorio en su agenda para iniciar el proceso de renovación necesario.

Le recomendamos que empiece con la renovación al menos un año antes del vencimiento de sus etiquetas TISAX.

Ahora que ya ha recibido sus etiquetas TISAX, puede proceder con el último paso y compartirlas con su socio.

6. Intercambio (paso 3)

El tiempo de lectura estimado de la sección de intercambio es de 7 minutos.

Ha recorrido el proceso TISAX, pero su socio todavía no ha visto ninguna “prueba” de que su sistema de gestión de la seguridad de la información es capaz de proteger sus datos confidenciales. Esta sección describe cómo compartir el resultado de la evaluación con su socio y presentar la prueba solicitada.

6.1. Premisa

Una de las características clave de TISAX es que el resultado de la evaluación está bajo su control. Sin su permiso explícito, la información relacionada con su evaluación no se comparte con nadie.

6.2. La plataforma de intercambio

El portal ENX alberga la plataforma de intercambio.

Su proveedor de auditoría subirá las dos primeras secciones (A y B) de su informe de evaluación TISAX. En esta fase, la información solo está disponible para usted.

Usted puede usar la cuenta que creó durante el registro para acceder al portal y usar la plataforma de intercambio.

Puede acceder al portal en esta dirección:
enx.com/en-US/SignIn

6.3. Requisitos previos generales

Puede compartir el resultado de la evaluación con sus socios solo si se cumplen estos dos requisitos previos:

1. Su proveedor de auditoría ha subido el resultado de la evaluación a la plataforma de intercambio.
   El resultado de la evaluación estará disponible en la plataforma de intercambio unos 5-10 días hábiles después de la emisión del informe de evaluación TISAX.
2. Hemos recibido su pago de la tasa (si procede).

El estado del alcance de la evaluación será “Activo” cuando se cumplen ambos requisitos previos.

Recuerde:

> Cada alcance de la evaluación tiene un ciclo de vida. Llegados a este punto, su alcance de la evaluación debe tener el estado “Activo”.
>
> Para más información sobre el estado de un alcance de la evaluación, consulte la Sección 7.5.5, “Assessment scope status “Awaiting your payment” (Estado del alcance de la evaluación “Pendiente de pago”)”.

Para comprobar si su resultado de la evaluación está listo para compartir (estado del alcance de la evaluación = Activo), siga estos pasos:

1. Inicie sesión en el portal ENX.
2. Vaya a la barra de navegación principal y seleccione “MY TISAX” (“MI TISAX”).
3. En el menú desplegable, seleccione “SCOPES AND ASSESSMENTS” (“ALCANCES Y EVALUACIONES”).
4. Vaya a la tabla y seleccione la fila con el alcance de la evaluación.
5. Compruebe que el alcance de la evaluación tiene el estado “Active” (“Activo”) (columna “Scope Status” (“Estado del alcance”)).

6.4. Permanencia de los resultados intercambiados

> Nota importante:
>
> No puede revocar los permisos de publicación o divulgación.
>
> El motivo de esto es que queremos que todos los participantes pasivos dispongan de un acceso continuo a cualquier resultado de evaluación que hayan recibido. De lo contrario, tendrían que gestionar y archivar los resultados de evaluación por su propia cuenta.
>
> El permiso seguirá siendo válido durante todo el periodo de validez de su evaluación TISAX.
>
> Si ha creado un permiso de publicación o divulgación por error, póngase en contacto con nosotros de inmediato.

6.5. Niveles de divulgación

Los niveles de divulgación equivalen a las secciones principales A-E del informe de evaluación TISAX.

	Secciones principales del informe de evaluación TISAX	Niveles de divulgación en la plataforma de intercambio
1	A. Información relacionada con la evaluación (Assessment Related Information)	
2	B. Resultados resumidos (Summarized Results)	
3	C. Resumen del resultado de la evaluación (Assessment result summary)	
4	D. Niveles de madurez de VDA ISA (pestaña de resultados) (Maturity Levels of VDA ISA (Result Tab))	
5	E. Resultados detallados de la evaluación (Detailed Assessment Results)	

Tabla 12. Secciones principales del informe de evaluación TISAX y niveles de divulgación en la plataforma de intercambio

Cuanto más alto es el nivel de divulgación, más detalles sobre su evaluación TISAX estarán disponibles para el correspondiente participante.

Para más detalles sobre el contenido de cada sección del informe de evaluación TISAX, consulte la Sección 5.4.7.4, “Informe de evaluación TISAX”.

6.6. Publicar el resultado de la evaluación en la plataforma de intercambio

Puede compartir el resultado de la evaluación con otros participantes de TISAX publicándolo en la plataforma de intercambio. De esta forma, el resto de participantes de TISAX podrán acceder al resultado de su evaluación hasta el nivel concedido.

Solo podrá publicar el resultado de su evaluación si el resultado global de la evaluación es “conforme”.

Los niveles de divulgación para publicar el resultado de evaluación en la plataforma de intercambio están limitados a estas opciones:

- Do not publish (Default) (No publicar (opción predeterminada))
- A. Assessment Related Information (A. Información relacionada con la evaluación)
- A + Labels (A + Etiquetas)
- A + Labels + B. Summarized Results (A + Etiquetas + B. Resultados resumidos)

Recomendamos el nivel de divulgación “A + Labels” (“A + Etiquetas”) para el tipo general de publicación.

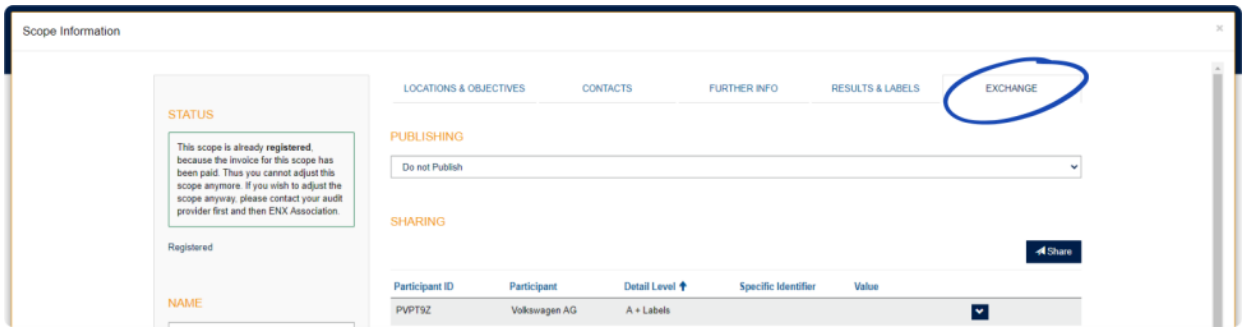
Nota importante:

Solo podrá publicar el resultado de la evaluación si se cumplen los requisitos

> previos descritos en la Sección 6.3, “Requisitos previos generales”.

Para publicar el resultado de la evaluación en la plataforma de intercambio, siga estos pasos:

1. Inicie sesión en el portal ENX.
2. Vaya a la barra de navegación principal y seleccione “MY TISAX” (“MI TISAX”).
3. En el menú desplegable, seleccione “SCOPES AND ASSESSMENTS” (“ALCANCES Y EVALUACIONES”).
4. Vaya a la tabla y seleccione la fila con el alcance de la evaluación.
5. Compruebe que el alcance de la evaluación tiene el estado “Active” (“Activo”) (columna “Scope Status” (“Estado del alcance”)).
6. Vaya al final de la fila de la tabla de su alcance de evaluación y haga clic en el botón con la flecha hacia abajo .
7. Seleccione “Scope Information” (“Información del alcance”).
8. En la nueva ventana (“Scope Information” (“Información del alcance”)), seleccione la pestaña “EXCHANGE” (“INTERCAMBIO”).



9. Vaya a la sección “PUBLISHING” (“PUBLICACIÓN”), abra el menú desplegable y seleccione el nivel de divulgación que desee (vea la recomendación anterior).

Recuerde:

Los resultados de la evaluación solo se publican en la plataforma de intercambio. Solo podrán acceder a ellos otros participantes de TISAX. No existe un listado público con todos los participantes de TISAX. En el sitio web público solo se menciona el número aproximado de participantes de TISAX.

6.7. Compartir el resultado de la evaluación con un participante concreto

Además de la opción mencionada anteriormente de publicar el resultado de la evaluación TISAX en la plataforma de intercambio, también puede compartirlo de forma selectiva con participantes de TISAX concretos con un nivel de divulgación superior.

A diferencia de la publicación mencionada anteriormente, podrá compartir el resultado de la evaluación incluso si el resultado global de la evaluación es no conforme (con una desviación mínima/importante).

Compartir los resultados de la evaluación es una parte fundamental de TISAX. Usted solo ha evaluado su sistema de gestión de la seguridad de la información una vez, pero ahora puede compartir el resultado de la evaluación con tantos socios como desee.

Las opciones para compartir el resultado de la evaluación en la plataforma de intercambio son:

1. A: Assessment Related Information (A: Información relacionada con la evaluación)
2. A + Labels (A + Etiquetas)
3. A + Labels + B: Assessment Summary (A + Etiquetas + B: Resumen de la evaluación)
4. A + Labels + B + C: Summarized Results (A + Etiquetas + B + C: Resultados resumidos)
5. A + Labels + B + C + D: Detailed Assessment Results (A + Etiquetas + B + C + D: Resultados detallados de la evaluación)
6. A + Labels + B + C + D + E: Maturity Levels according to ISA (A + Etiquetas + B + C + D + E: Niveles de madurez según la ISA)

Recomendamos el nivel de divulgación “A + Labels” (“A + Etiquetas”). Este nivel es suficiente para la mayoría de socios. Siempre podrá seleccionar un nivel de divulgación superior más tarde.

Recuerde:

Algunos participantes de TISAX procesan los resultados de evaluación de sus socios automáticamente. A tal fin, sincronizan su propio sistema con el portal ENX. Solo se sincronizarán los resultados de evaluación compartidos específicamente con dichos participantes. Su mera publicación, como se describe anteriormente en la Sección 6.6, “Publicar el resultado de la evaluación en la plataforma de intercambio”, no se reconocerá.

Entre los OEM que usan TISAX, BMW es un ejemplo de este procedimiento. Si usted es socio de BMW, asegúrese de compartir (y no solo de publicar) el resultado de su evaluación con BMW.

6.7.1. Requisitos previos

Estos son los requisitos previos para compartir el resultado de su evaluación con su socio (o cualquier otro participante de TISAX):

- Solo puede compartir el resultado de la evaluación TISAX con otros participantes de TISAX.
- Su socio tiene que ser un participante de TISAX.

- Usted necesitará el ID de participante de su socio.[31]
- Tiene que pagar la tasa (si procede).

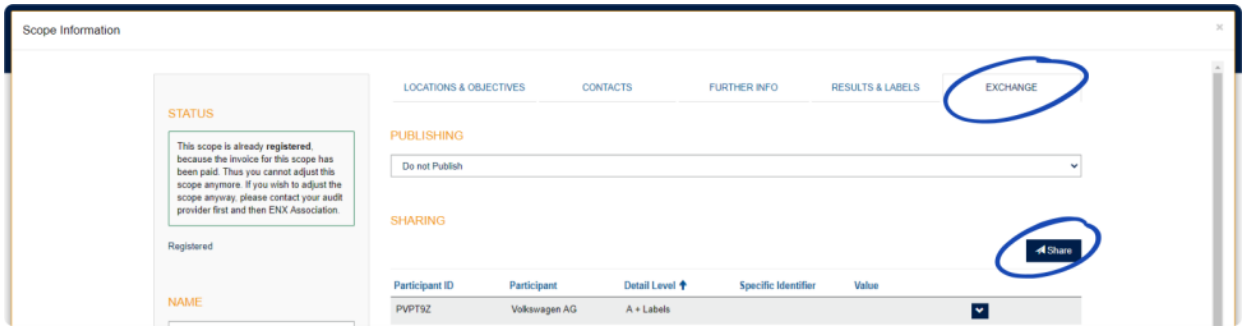
Nota importante:

Solo podrá compartir el resultado de la evaluación si se cumplen los requisitos generales descritos en la Sección 6.3, “Requisitos previos generales”.

6.7.2. Cómo crear permisos de divulgación

Para compartir el resultado de la evaluación con otros participantes de TISAX siga estos pasos:

1. Inicie sesión en el portal ENX.
2. Vaya a la barra de navegación principal y seleccione “MY TISAX” (“MI TISAX”).
3. En el menú desplegable, seleccione “SCOPES AND ASSESSMENTS” (“ALCANCES Y EVALUACIONES”).
4. Vaya a la tabla y seleccione la fila con el alcance de la evaluación.
5. Compruebe que el alcance de la evaluación tiene el estado “Active” (“Activo”) (columna “Scope Status” (“Estado del alcance”)).
6. Vaya al final de la fila de la tabla de su alcance de evaluación y haga clic en el botón con la flecha hacia abajo .
7. Seleccione “Scope Information” (“Información del alcance”).
8. En la nueva ventana (“Scope Information” (“Información del alcance”)), seleccione la pestaña “EXCHANGE” (“INTERCAMBIO”).



9. Vaya a la sección “SHARING” (“DIVULGACIÓN”) y haga clic en el botón “Share” (“Compartir”).
10. En la nueva ventana (“SHARE THIS SCOPE” (“COMPARTIR ESTE ALCANCE”)), introduzca el ID de participante de su socio (o selecciónelo en la lista de participantes disponible en el cuadro de búsqueda de al lado).
11. Seleccione el nivel de divulgación que desee.
12. Haga clic en el botón “Next” (“Siguiente”).

13. Lea y entienda las instrucciones sobre la permanencia del permiso de divulgación.
14. Marque las dos casillas de verificación “confirm” (“confirmar”).
15. Haga clic en el botón “Submit” (“Enviar”).

Del resto se ocupa la plataforma de intercambio. Para los niveles de divulgación A y B, la información estará disponible en la plataforma de intercambio. Su socio podrá iniciar sesión en el portal ENX y ver el resultado de la evaluación que usted ha compartido[32].

Para los niveles de divulgación superiores (C-E), la plataforma de intercambio notificará a su proveedor de auditoría. A continuación, el proveedor de auditoría enviará la información (de acuerdo con el nivel de divulgación seleccionado) al contacto principal del participante estipulado por su socio.

6.8. Compartir el resultado de la evaluación fuera de TISAX

La norma[33] establece que usted puede usar la plataforma de intercambio TISAX únicamente para dar a conocer a otros participantes de TISAX el resultado de su evaluación.

6.8.1. Las razones de este estricto mecanismo de intercambio

TISAX proporciona un mecanismo estandarizado de intercambio de los resultados de evaluación. Esto ofrece un valor añadido en comparación con el intercambio de los resultados de otras certificaciones (p. ej., ISO), que se lleva a cabo de formas distintas y que no siempre incluye toda la información necesaria para tener una imagen completa.

Los OEM valoran especialmente esta estandarización. Pero otras empresas también se benefician de procedimientos claramente definidos.

6.8.2. Una guía para escribir en público sobre TISAX

Si bien no puede hablar públicamente de los resultados de su evaluación, sí puede mencionar sus esfuerzos relacionados con TISAX. En el portal ENX proporcionamos consejos sobre cómo llevar a cabo declaraciones públicas. También proporcionamos logotipos TISAX que puede utilizar.

Tras iniciar sesión en el portal ENX, puede acceder a la información aquí:
enx.com/en-US/myenxportal/marketing/
Descarga directa de archivo ZIP (documento y logotipos):
enx.com/en-US/myenxportal/marketing/TISAX-Trademark-and-Logos-Terms-and-Conditions.zip

En caso de que se esté preguntando si existe un certificado que pueda colgar en la pared: Debido al proceso de intercambio estandarizado mencionado arriba, no proporcionamos ese

tipo de certificado.

6.8.3. Cómo compartir el resultado con un socio que todavía no es participante de TISAX

Si quiere compartir el resultado de su evaluación TISAX con un socio en particular que a) todavía no es participante de TISAX y b) todavía no ha recibido etiquetas TISAX (después de superar el proceso de evaluación), puede seguir estos pasos:

1. Indique a su socio que se registre como participante de TISAX.
   Solo tiene que registrarse como participante de TISAX. No es necesario que registre un alcance de evaluación.
2. Indique a su socio que se ponga en contacto con nosotros.
   Normalmente, solo procesamos un nuevo registro si la empresa también registra un alcance de evaluación. Si lo solicita su socio, procesaremos su registro. De esta forma, se convertirá en un participante de TISAX. Ahora ya podrá recibir el resultado de su evaluación TISAX a través del proceso de intercambio habitual.

El objetivo de este proceso es asegurar que el socio observará las “Condiciones generales de participación en TISAX” que rigen el intercambio de los resultados de la evaluación TISAX.

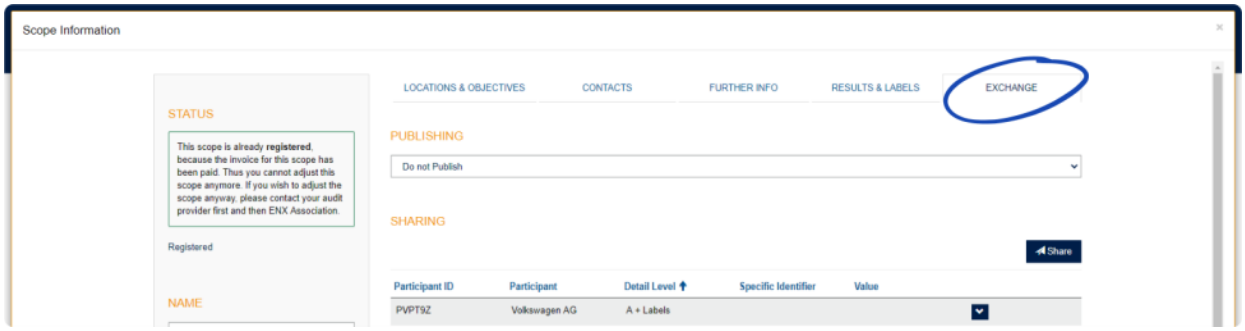
Solo se incurre en costes si se registra un alcance de evaluación. Por tanto, dado que registrarse como participante de TISAX es gratuito, su socio podrá recibir el resultado de su evaluación sin coste. No obstante, si su socio no dispone de su propio resultado de evaluación, solo podrá recibir hasta cinco resultados de evaluación y no podrá ver las publicaciones.

6.8.4. Cómo compartir el resultado con empleados de su socio que no tienen acceso directo al portal ENX

Solo aquellos empleados de su socio que tengan una cuenta en nuestro portal ENX podrán ver directamente su resultado. Si ha de mostrar etiquetas TISAX a un empleado de su socio sin acceso al portal, podrá usar un documento PDF especial con este fin. Para obtener el documento, siga los siguientes pasos:

1. Comparta el resultado de la evaluación con su socio como se describe en la Sección 6.7, “Compartir el resultado de la evaluación con un participante concreto”.
2. Inicie sesión en el portal ENX.
3. Vaya a la barra de navegación principal y seleccione “MY TISAX” (“MI TISAX”).
4. En el menú desplegable, seleccione “SCOPES AND ASSESSMENTS” (“ALCANCES Y EVALUACIONES”).
5. Vaya a la tabla y seleccione la fila con el alcance de la evaluación.
6. Compruebe que el alcance de la evaluación tiene el estado “Active” (“Activo”) (columna “Scope Status” (“Estado del alcance”)).

7. Vaya al final de la fila de la tabla de su alcance de evaluación y haga clic en el botón con la flecha hacia abajo .
8. Seleccione “Scope Information” (“Información del alcance”).
9. En la nueva ventana (“Scope Information” (“Información del alcance”)), seleccione la pestaña “EXCHANGE” (“INTERCAMBIO”).



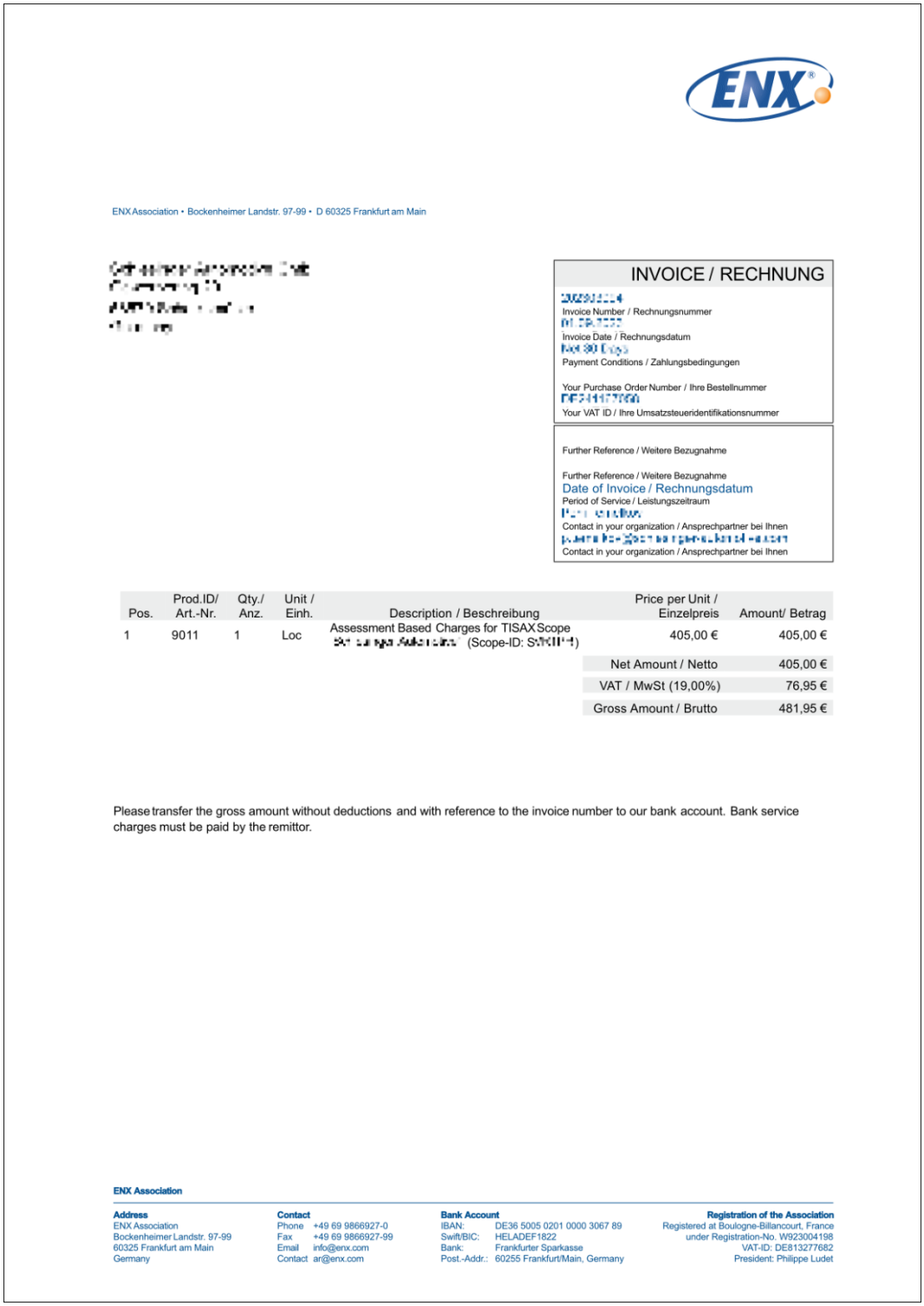
10. Vaya al apartado “SHARING” (“DIVULGACIÓN”) y localice la fila de la tabla con el permiso de divulgación (como se había creado en el paso 1).
11. Vaya al final de la fila de la tabla de su permiso de divulgación y haga clic en el botón con la flecha hacia abajo .
12. Seleccione “Edit” (“Editar”)
13. En la nueva ventana (“SHARE THIS SCOPE” (“COMPARTIR ESTE ALCANCE”)), desplácese hasta la parte inferior y seleccione “Request Shared Information as PDF” (“Solicitar información compartida como PDF”).
14. Espere un momento hasta que se genere el documento.
15. Descargue el documento (“Copy of information shared with ACME.pdf (66.84 KB)” (“Copia de la información compartida con ACME.pdf (66,84 KB)”))

7. Anexos

7.1. Anexo: Ejemplo de factura

Este es un ejemplo de la factura que enviamos.

Para más información, consulte la Sección 4.3.4, “Tasa”.



ENX Association • Bockenheimer Landstr. 97-99 • D 60325 Frankfurt am Main

[redacted]

INVOICE / RECHNUNG

[redacted]
Invoice Number / Rechnungsnummer
[redacted]
Invoice Date / Rechnungsdatum
[redacted]
Payment Conditions / Zahlungsbedingungen

Your Purchase Order Number / Ihre Bestellnummer
[redacted]
Your VAT ID / Ihre Umsatzsteueridentifikationsnummer

Further Reference / Weitere Bezugnahme

Further Reference / Weitere Bezugnahme
Date of Invoice / Rechnungsdatum
Period of Service / Leistungszeitraum
[redacted]
Contact in your organization / Ansprechpartner bei Ihnen
[redacted]
Contact in your organization / Ansprechpartner bei Ihnen

Pos.	Prod.ID/ Art.-Nr.	Qty./ Anz.	Unit / Einh.	Description / Beschreibung	Price per Unit / Einzelpreis	Amount/ Betrag
1	9011	1	Loc	Assessment Based Charges for TISAX Scope [redacted] (Scope-ID: [redacted])	405,00 €	405,00 €
					Net Amount / Netto	405,00 €
					VAT / MwSt (19,00%)	76,95 €
					Gross Amount / Brutto	481,95 €

Please transfer the gross amount without deductions and with reference to the invoice number to our bank account. Bank service charges must be paid by the remittor.

ENX Association

Address	Contact	Bank Account	Registration of the Association
ENX Association Bockenheimer Landstr. 97-99 60325 Frankfurt am Main Germany	Phone +49 69 9866927-0 Fax +49 69 9866927-99 Email info@enx.com Contact ar@enx.com	IBAN: DE36 5005 0201 0000 3067 89 Swift/BIC: HELADEF1822 Bank: Frankfurter Sparkasse Post.-Addr.: 60255 Frankfurt/Main, Germany	Registered at Boulogne-Billancourt, France under Registration-No. W923004198 VAT-ID: DE813277682 President: Philippe Ludet

7.2. Anexo: Ejemplo de mensaje de correo electrónico de confirmación

Le enviaremos el mensaje electrónico de confirmación una vez que haya completado todos los pasos obligatorios durante el proceso de registro online.

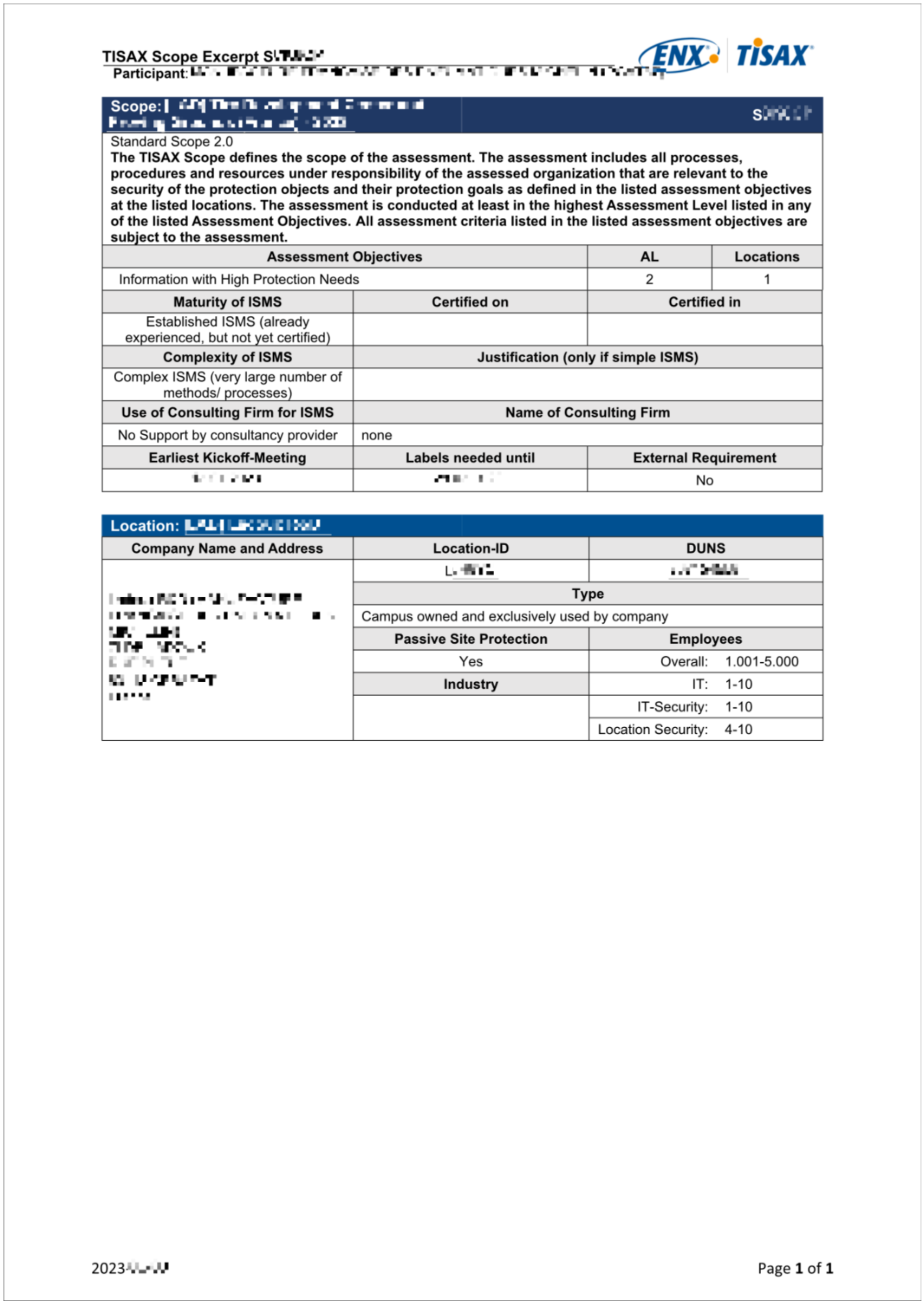
Para más información sobre cuándo enviamos el mensaje de correo electrónico de confirmación, consulte la Sección 4.5.8, “Mensaje de correo electrónico de confirmación”.

```
Asunto: [TISAX] Alcance S3ZY5V aprobado

Hola, John Doe:

Gracias por registrar el alcance de la evaluación TISAX. Acabo de registrar y
aprobar su alcance. En el anexo encontrará el TISAX Scope Excerpt, incluidas la
información sobre el alcance y la lista actual de proveedores de auditoría TISAX.

¿Cuál es el siguiente paso?

Con el TISAX Scope Excerpt adjunto, puede solicitar presupuestos para su alcance a
todos los proveedores de auditoría TISAX.

¿Necesita ayuda?

Si tiene más preguntas sobre TISAX, lea las preguntas frecuentes de TISAX o el
Manual del participante de TISAX. Si necesita más ayuda para el proceso TISAX, no
dude en ponerse en contacto con nuestra línea directa TISAX por correo electrónico
(tisax@enx.com) o teléfono (+49 69 986692-777).

Atentamente,

Su equipo de TISAX
```

7.3. Anexo: Ejemplo de TISAX Scope Excerpt

Recibirá el “TISAX Scope Excerpt” adjunto al mensaje de correo electrónico de confirmación.

Para más información, consulte la Sección 4.5.8, “Mensaje de correo electrónico de confirmación”.



TISAX Scope Excerpt S[redacted]

Participant: [redacted]

Scope: [redacted]

Standard Scope 2.0

The TISAX Scope defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations. The assessment is conducted at least in the highest Assessment Level listed in any of the listed Assessment Objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.

Assessment Objectives	AL	Locations
Information with High Protection Needs	2	1

Maturity of ISMS	Certified on	Certified in
Established ISMS (already experienced, but not yet certified)		

Complexity of ISMS	Justification (only if simple ISMS)
Complex ISMS (very large number of methods/ processes)	

Use of Consulting Firm for ISMS	Name of Consulting Firm
No Support by consultancy provider	none

Earliest Kickoff-Meeting	Labels needed until	External Requirement
[redacted]	[redacted]	No

Location: [redacted]

Company Name and Address	Location-ID	DUNS
[redacted]	[redacted]	[redacted]
	Type	
	Campus owned and exclusively used by company	
	Passive Site Protection	**Employees**
	Yes	Overall: 1.001-5.000
	Industry	IT: 1-10
		IT-Security: 1-10
		Location Security: 4-10

2023[redacted]

Page **1** of **1**

7.4. Anexo: Participant status (Estado del participante)

7.4.1. Sinopsis: Participant status (Estado del participante)

El “estado del participante” define en qué punto se encuentra (como empresa) dentro del proceso TISAX.

Su “estado del participante” puede ser:

1. Incomplete (Incompleto)
2. Awaiting approval (Pendiente de aprobación)
3. Preliminary (Preliminar)
4. Registered (Registrado)
5. Expired (Expirado)

Las siguientes tablas relativas a los estados describen:

- su situación
  (su situación real en este momento cuando tiene este estado)
- su próxima acción
  (lo que debe hacer para avanzar al siguiente estado, si procede)
- nuestra próxima acción
  (lo que tenemos que hacer nosotros para aumentar su estado, si procede)
- el siguiente estado
  (si procede)

La siguiente ilustración muestra las acciones que llevan a avanzar de un estado al siguiente:

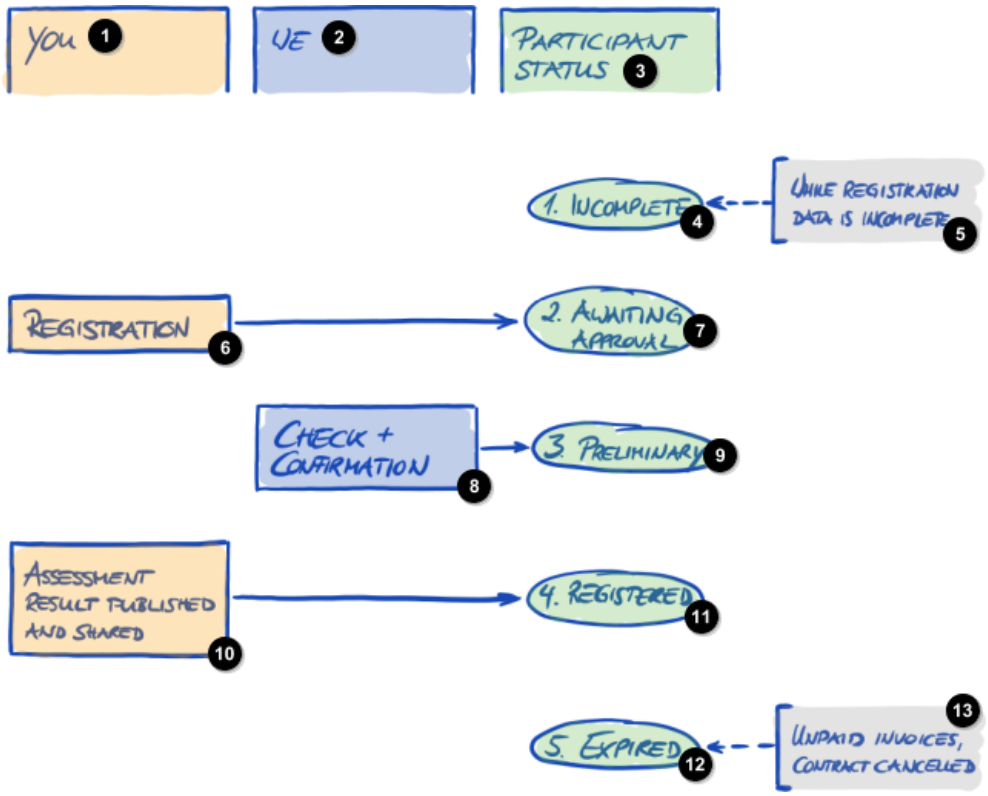


Figura 34. Sinopsis de estados del participante

1. Usted
2. Nosotros
3. Estado del participante
4. 1. Incompleto
5. Con los datos de registro todavía incompletos
6. Registro
7. 2. Pendiente de aprobación
8. Comprobación + confirmación
9. 3. Preliminar
10. Resultado de la evaluación publicado y compartido
11. 4. Registrado
12. 5. Expirado
13. Facturas sin pagar, contrato cancelado

7.4.2. Participant status “Incomplete” (Estado del participante “Incompleto”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Incompleto	No ha completado el registro TISAX. O bien no ha aceptado las condiciones generales. O no ha especificado la ubicación principal del participante. O no ha asignado el contacto principal del participante. O falta otra información necesaria.	Continúe en enx.com/en-US/SignIn	Le enviaremos un recordatorio por correo electrónico (habitualmente en unos días).	Pendiente de aprobación

7.4.3. Participant status “Awaiting approval” (Estado del participante “Pendiente de aprobación”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Pendiente de aprobación	Su registro TISAX está completo. Tal vez ya ha registrado el alcance de la evaluación o no.	Espere a nuestra próxima acción.	Comprobaremos su solicitud y normalmente la aprobaremos. No obstante, si registra un alcance de evaluación, pondrá en marcha nuestra comprobación. Asignaremos un ID de participante y el o los ID de alcance. Le enviaremos un mensaje de correo electrónico de confirmación. El “TISAX Scope Excerpt” (PDF) adjunto resume la información que tenemos en la base de datos.	Preliminar

7.4.4. Participant status “Preliminary” (Estado del participante “Preliminar”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Preliminar	Ha finalizado correctamente el proceso de registro TISAX.	Pagar la tasa (si procede). Llevar a cabo el proceso de evaluación TISAX. Publicar y compartir el resultado de la evaluación.	Ninguna	Registrado

7.4.5. Participant status “Registered” (Estado del participante “Registrado”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Registrado	Ha completado correctamente el proceso de evaluación TISAX y ha recibido las etiquetas TISAX. Ha publicado y compartido el resultado de la evaluación. Solo recibirá etiquetas TISAX cuando haya superado el proceso de evaluación TISAX. En el portal ENX, esto se refleja con el estado “Activo” del alcance de la evaluación.	Ninguna	Ninguna	(Expirado)

Recuerde:

Si quiere acceder a los resultados de la evaluación de su(s) socio(s):

El requisito previo para poder recibir resultados de evaluación de otros participantes es:

- Usted comparte sus propios resultados de evaluación (esto “prueba” que es un participante de TISAX serio y un miembro de la comunidad del automóvil).
- Le reconocemos por su reputación en el sector del automóvil (como a los OEM o proveedores tier 1).
- Usted demuestra que tiene un interés legítimo en recibir resultados de evaluación de otros participantes. Tendremos que verificarlo mediante un proceso elaborado que puede suponer una tasa sustancial. Para más información, póngase en contacto con nosotros.

7.4.6. Participant status “Expired” (Estado del participante “Expirado”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Expirado	No ha pagado la tasa. O bien se ha rescindido el contrato (las Condiciones generales).	Ninguna	Ninguna	n/a

7.5. Anexo: Assessment scope status (Estado del alcance de la evaluación)

7.5.1. Sinopsis: Assessment scope status (Estado del alcance de la evaluación)

El “estado del alcance de la evaluación” define en qué punto se encuentra su alcance de evaluación dentro de su ciclo de vida.

Tenga en cuenta que el “estado del alcance de la evaluación” es diferente al “estado de la evaluación”. Para más información sobre el “estado de la evaluación”, consulte la Sección 7.6, “Anexo: Assessment status (Estado de la evaluación)”.

Su “estado del alcance de la evaluación” puede ser:

1. Incomplete (Incompleto)
2. Awaiting your order (Pendiente del pedido)
3. Awaiting ENX approval (Pendiente de aprobación ENX)
4. Awaiting your payment (Pendiente de pago)
5. Registered (Registrado)
6. Active (Activo)
7. Expired (Expirado)

Las siguientes tablas relativas a los estados describen:

- su situación
  (su situación real en este momento cuando tiene este estado)
- su próxima acción
  (lo que debe hacer para avanzar al siguiente estado, si procede)

- nuestra próxima acción
  (lo que tenemos que hacer nosotros para aumentar su estado, si procede)
- el siguiente estado
  (si procede)

La siguiente ilustración muestra las acciones que llevan a avanzar de un estado al siguiente:

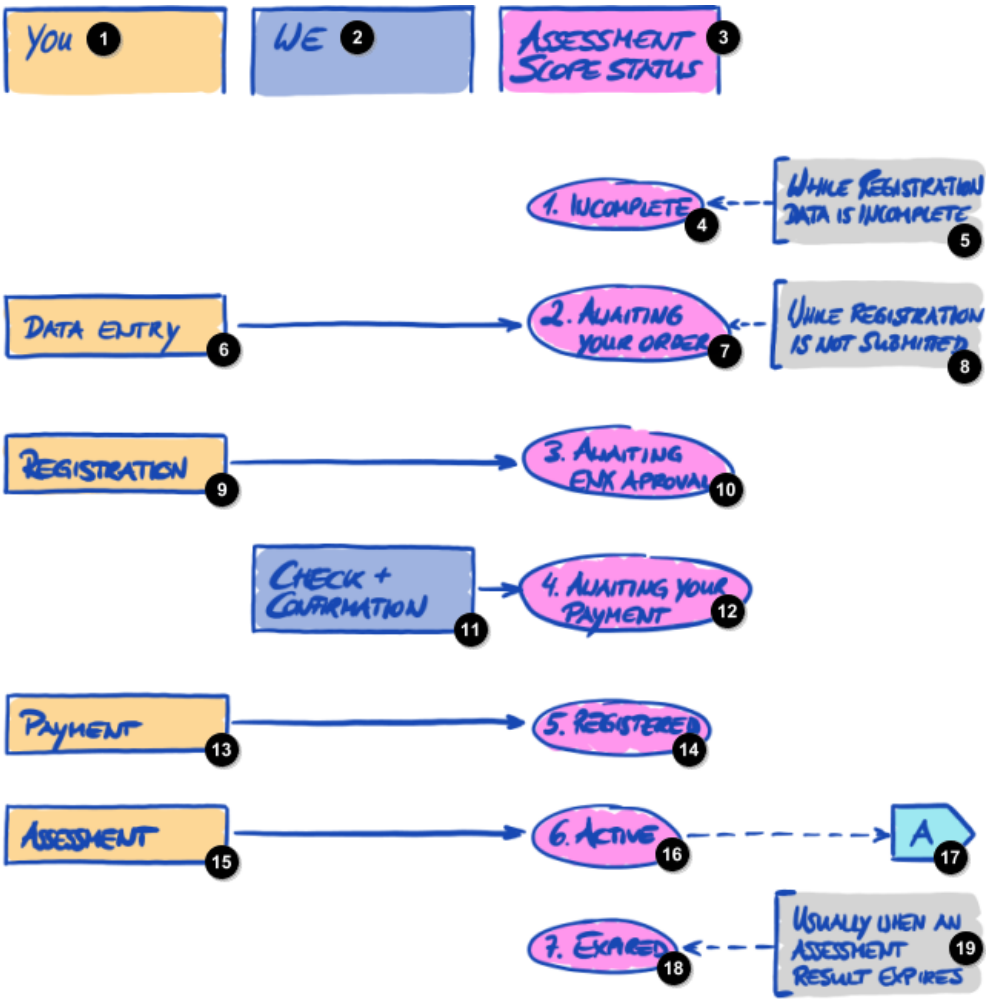


Figura 35. Sinopsis de estados del alcance de la evaluación

1. Usted
2. Nosotros
3. Estado del alcance de la evaluación
4. 1. Incompleto
5. Con los datos de registro todavía incompletos
6. Entrada de datos
7. 2. Pendiente del pedido

8. Mientras no se envíe el registro
9. Registro
10. 3. Pendiente de aprobación ENX
11. Comprobación + confirmación
12. 4. Pendiente de pago
13. Pago
14. 5. Registrado
15. Evaluación
16. 6. Activo
17. A
18. 7. Expirado
19. Habitualmente, cuando vence un resultado de evaluación

La referencia “A” a otra página de la figura superior conecta el estado del alcance de la evaluación “Activo” con el “estado de la evaluación”. Para más información sobre el “estado de la evaluación”, consulte la Sección 7.6, “Anexo: Assessment status (Estado de la evaluación)”.

7.5.2. Assessment scope status “Incomplete” (Estado del alcance de la evaluación “Incompleto”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Incompleto	O bien no ha completado el registro del alcance de la evaluación. O bien no ha facilitado toda la información necesaria.	Continúe en enx.com/en-US/SignIn	Le enviaremos un recordatorio por correo electrónico (habitualmente en unos días).	Pendiente del pedido

Para más información sobre el impacto de este estado, consulte la Sección 4.5.7, “Registro del alcance de la evaluación”.

7.5.3. Assessment scope status “Awaiting your order” (Estado del alcance de la evaluación “Pendiente del pedido”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Pendiente del pedido	No ha finalizado el registro de su alcance.	Continúe en enx.com/en-US/SignIn	Le enviaremos un recordatorio por correo electrónico (habitualmente en unos días).	Pendiente de aprobación ENX

Para más información sobre el impacto de este estado, consulte la Sección 4.5.7, “Registro del alcance de la evaluación”.

7.5.4. Assessment scope status “Awaiting ENX approval” (Estado del alcance de la evaluación “Pendiente de aprobación ENX”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Pendiente de aprobación ENX	Su registro del alcance de la evaluación está completo.	Espere a nuestra próxima acción.	Comprobaremos su solicitud y normalmente la aprobaremos. Asignaremos el o los ID de alcance. Le enviaremos un mensaje de correo electrónico de confirmación. El “TISAX Scope Excerpt” (PDF) adjunto resume la información que tenemos en la base de datos.	Pendiente de pago

Para más información sobre el impacto de este estado, consulte la Sección 4.5.7, “Registro del alcance de la evaluación”.

7.5.5. Assessment scope status “Awaiting your payment” (Estado del alcance de la evaluación “Pendiente de pago”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Pendiente de pago	Su registro del alcance de la evaluación está completo y aprobado. Ha recibido el mensaje de correo electrónico de confirmación y el “TISAX Scope Excerpt”.	Pagar la tasa (si procede). Solicitar ofertas a nuestros proveedores de auditoría TISAX. A partir del estado “Pendiente de pago”, usted: ▪ puede empezar a compartir con su socio información relativa a la evaluación. [34] ▪ puede preconfigurar la publicación del resultado de su evaluación (que solo será efectiva una vez que el estado del alcance de la evaluación cambie a “Activo”.	A la espera del pago por su parte.	Registrado

Para más información sobre el impacto de este estado, consulte la Sección 4.5.8, “Mensaje de correo electrónico de confirmación”.

7.5.6. Assessment scope status “Registered” (Estado del alcance de la evaluación “Registrado”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Registrado	Su alcance de la evaluación está registrado. Hemos recibido el pago completo o su estado comercial es “verde” por otros motivos.	Llevar a cabo el proceso de evaluación TISAX.	Ninguna	Activo

7.5.7. Assessment scope status “Active” (Estado del alcance de la evaluación “Activo”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Activo	Ha completado correctamente el proceso de evaluación TISAX y ha recibido las etiquetas TISAX.	Publicar y compartir el resultado de la evaluación. Cualquier permiso de publicación o divulgación preconfigurado en un estado inferior se vuelve efectivo.	Ninguna	Expirado

Para más información sobre publicar y compartir, consulte la Sección 6, “Intercambio (paso 3)”.

7.5.8. Assessment scope status “Expired” (Estado del alcance de la evaluación “Expirado”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Expirado	O bien: ▪ no ha completado el registro del alcance de la evaluación en 90 días,	Iniciar un nuevo registro del alcance de la evaluación.	Ninguna	Incompleto o bien Pendiente del pedido o bien Pendiente de aprobación ENX
	• o bien se ha producido un retraso con el pago de la tasa,			
	• o ha abandonado el proceso TISAX,			
	• o la validez del resultado de su evaluación ha vencido (tres años),			
	• o ha tenido cambios significativos en el alcance de la evaluación (ejemplo: las ubicaciones dentro del alcance de la evaluación ya no son de su empresa).			

7.6. Anexo: Assessment status (Estado de la evaluación)

7.6.1. Sinopsis: Assessment status (Estado de la evaluación)

El “estado de la evaluación” define en qué punto se encuentra dentro del proceso de evaluación. El estado cambia a medida que progresa de un tipo de evaluación al siguiente (por ejemplo, de “evaluación inicial” a “evaluación del plan de acciones correctivas”).

Tenga en cuenta que el “estado de la evaluación” es diferente al “estado del alcance de la evaluación”. Para más información sobre el “estado del alcance de la evaluación”, consulte la Sección 7.5, “Anexo: Assessment scope status (Estado del alcance de la evaluación)”.

Su “estado de la evaluación” puede ser:

1. Initial assessment ordered (Evaluación inicial solicitada)
2. Initial assessment ongoing (Evaluación inicial en curso)
3. Waiting for corrective action plan assessment (A la espera de la evaluación del plan de acciones correctivas)
4. Waiting for follow-up (A la espera del seguimiento)
5. Finished (Finalizado)

Las siguientes tablas relativas a los estados describen:

- su situación
  (su situación real en este momento cuando tiene este estado)
- su próxima acción
  (lo que debe hacer para avanzar al siguiente estado, si procede)
- nuestra próxima acción
  (lo que tenemos que hacer nosotros para aumentar su estado, si procede)
- el siguiente estado
  (si procede)

La siguiente ilustración muestra las acciones que llevan a avanzar de un estado al siguiente:

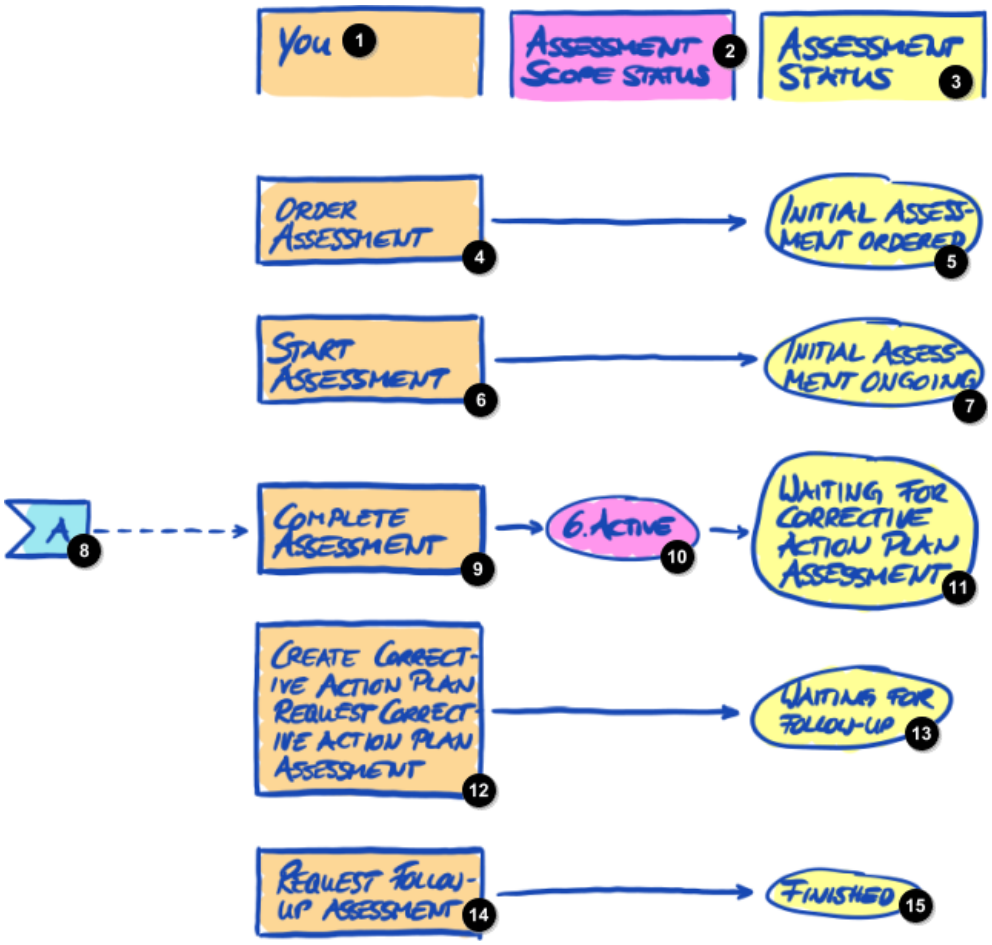


Figura 36. Sinopsis de estados de la evaluación

1. Usted
2. Estado del alcance de la evaluación
3. Estado de la evaluación
4. Solicitar la evaluación
5. Evaluación inicial solicitada
6. Iniciar la evaluación
7. Evaluación inicial en curso
8. A
9. Completar la evaluación
10. 6. Activo
11. A la espera de la evaluación del plan de acciones correctivas
12. Crear el plan de acciones correctivas
    Solicitar la evaluación del plan de acciones correctivas

13. A la espera del seguimiento
14. Solicitar la evaluación de seguimiento
15. Finalizado

La referencia “A” a otra página de la figura superior conecta el estado del alcance de la evaluación “Activo” con el estado de la evaluación “A la espera de la evaluación del plan de acciones correctivas”. Para más información sobre el “estado del alcance de la evaluación”, consulte la Sección 7.5, “Anexo: Assessment scope status (Estado del alcance de la evaluación)”.

7.6.2. Assessment status “Initial assessment ordered” (Estado de la evaluación “Evaluación inicial solicitada”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Evaluación inicial solicitada	Ha seleccionado uno de nuestros proveedores de auditoría TISAX y ha solicitado una evaluación inicial.	Continuar con el proceso de evaluación TISAX.	Ninguna	Evaluación inicial en curso

7.6.3. Assessment status “Initial assessment ongoing” (Estado de la evaluación “Evaluación inicial en curso”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Evaluación inicial en curso	Su evaluación inicial: ▪ ha empezado ▪ o se ha completado, pero el proveedor de auditoría todavía no ha emitido el informe de evaluación TISAX	Ninguna	Ninguna	A la espera de la evaluación del plan de acciones correctivas (si procede)

7.6.4. Assessment status “Waiting for corrective action plan assessment” (Estado de la evaluación “A la espera de la evaluación del plan de acciones correctivas”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
A la espera de la evaluación del plan de acciones correctivas	Su proveedor de auditoría ha realizado la evaluación inicial. Su proveedor de auditoría nos ha enviado el informe de evaluación TISAX. El resultado de la evaluación es no conforme (con una desviación mínima/importante).	Crear un plan de acciones correctivas. Iniciar las acciones correctivas. Solicitar una evaluación del plan de acciones correctivas.	Ninguna	A la espera del seguimiento (si procede)

El estado de la evaluación “A la espera de la evaluación del plan de acciones correctivas” está limitado a nueve meses. Para más información, consulte la Sección 5.4.9.3, “Requisitos del plan de acciones correctivas”.

7.6.5. Assessment status “Waiting for follow-up” (Estado de la evaluación “A la espera del seguimiento”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
A la espera del seguimiento	Su proveedor de auditoría ha aprobado el plan de acciones correctivas. Usted ha implementado las acciones correctivas.	Solicitar una evaluación de seguimiento.	Ninguna	Finalizado

El estado de la evaluación “A la espera del seguimiento” está limitado a nueve meses. Para más información, consulte la Sección 5.4.9.3, “Requisitos del plan de acciones correctivas”.

7.6.6. Assessment status “Finished” (Estado de la evaluación “Finalizado”)

Estado	Situación	Su próxima acción	Nuestra próxima acción	Siguiente estado
Finalizado	Su proveedor de auditoría ha realizado una evaluación de seguimiento. El resultado de la evaluación no tiene no conformidades. Su proveedor de auditoría nos ha enviado el informe de evaluación TISAX.	Publicar y compartir el resultado de la evaluación.	Ninguna	n/a

7.7. Anexo: El razonamiento en contra de las “pre-evaluaciones” y los “análisis de deficiencias”

Habitualmente, recomendamos no solicitar al proveedor de auditoría que lleve a cabo una “pre-evaluación” o “análisis de deficiencias”. En la mayoría de los casos, tiene más sentido iniciar el proceso de evaluación TISAX directamente.

En esta sección abordamos las dudas más comunes.

¿Está pensando en una pre-evaluación porque…?

1. ¿Le preocupa que su cliente pueda ver un resultado de evaluación potencialmente desfavorable?

   Usted tiene pleno control sobre quién ve los resultados de su evaluación. Usted decide si el proveedor de auditoría carga algo en el portal ENX. Si nadie debe verlo, nadie lo verá (excepto el auditor, claro).

   Además, el proveedor de auditoría solo carga las dos primeras secciones del informe de evaluación TISAX y *nunca* carga los resultados detallados de la evaluación.

2. ¿Cree que una pre-evaluación le ahorrará dinero?
   - Con una pre-evaluación:

- pagará por la pre-evaluación
- pagará por los posibles costes internos de arreglar cualquier no conformidad
- pagará por la evaluación TISAX completa (“evaluación inicial”)

Incluso si *no* hay hallazgos, siempre paga por *dos* evaluaciones completas.

- Si empieza con una evaluación TISAX:
  - pagará por la “evaluación inicial”
  - pagará por los posibles costes internos de arreglar cualquier no conformidad
  - puede pagar mucho menos (en comparación con la evaluación inicial) por la llamada “evaluación de seguimiento”, en la que el auditor solo se centra en si ha solucionado las no conformidades de la evaluación inicial

  Incluso *con* hallazgos, solo pagará por una evaluación completa más la breve evaluación de seguimiento.

3. ¿Cree que podría suspender la evaluación con consecuencias permanentes?

   No puede suspender de forma permanente, porque puede tener tantas evaluaciones como quiera. Si el resultado de la evaluación no cumple sus expectativas o si no consigue solucionar las no conformidades con acciones correctivas en el plazo requerido de nueve meses, simplemente puede considerar el intento fallido como una pre-evaluación y empezar de nuevo. Y nadie tiene por qué ver los resultados del primer intento. Puede compartir únicamente el resultado de la evaluación superada.

Otras consideraciones:

- Si el resultado de la evaluación es mejor de lo esperado, puede llegar a recibir etiquetas temporales TISAX. Podría compartirlas directamente con su socio. Esto no es posible con una pre-evaluación.
- Si el proveedor de auditoría que realiza la pre-evaluación debe realizar también la evaluación TISAX, dicho auditor no podrá consultarle. De lo contrario, deberá elegir a otro proveedor de auditoría para la evaluación TISAX.

Aunque la mayoría de empresas auditadas no se benefician de una pre-evaluación, queremos mencionar las siguientes ventajas.

El auditor:

- se puede centrar en los aspectos críticos de su ISMS
- puede dedicar más tiempo del habitual y analizar en mayor profundidad
- puede documentar los hallazgos de forma diferente

Después de leer las secciones sobre el proceso de evaluación TISAX, le resultará aún más fácil comprender nuestro razonamiento.

7.8. Anexo: Alcances personalizados

Casi todos los participantes de TISAX eligen el alcance estándar. No obstante, en *raras* ocasiones, puede necesitar un alcance personalizado.

Existen dos tipos de alcance personalizado:

7.8.1. Alcance ampliado personalizado

Puede ampliar el alcance. Un alcance ampliado personalizado abarca MÁS que el alcance estándar. El proveedor de auditoría llevará a cabo más comprobaciones.

Finalidad: Un alcance ampliado personalizado puede ser relevante si quiere utilizar la evaluación TISAX con fines internos o fuera de la industria automovilística.

Etiquetas TISAX y divulgación de los resultados: Un alcance ampliado personalizado siempre incluye el alcance estándar. Por tanto, un alcance ampliado personalizado recibirá etiquetas TISAX[35]. Otros participantes de TISAX también aceptarán el resultado de la evaluación.

Descripción: Mientras que el alcance estándar tiene una descripción predefinida, si necesita un alcance ampliado personalizado deberá redactar su propia descripción del alcance.

7.8.2. Alcance completamente personalizado

También puede definir completamente su propio alcance.

Finalidad: Si tiene ubicaciones que pertenecen a distintos alcances de evaluación y que usan servicios de una sede en concreto (como un centro de datos), puede utilizar un alcance completamente personalizado para esos servicios. De esta forma, el proveedor de auditoría TISAX puede reutilizar fácilmente el resultado de la evaluación del alcance completamente personalizado del servicio.

Ejemplo: Usted tiene varias ubicaciones (posiblemente parte de distintos alcances) y tiene un departamento de TI central en una de esas ubicaciones. Definir un alcance completamente personalizado solo para el departamento de TI permite reutilizar el correspondiente resultado de la evaluación en los otros alcances.

Etiquetas TISAX y divulgación de los resultados: Los alcances completamente personalizados no obtienen etiquetas TISAX. El resultado de su evaluación se registra en el portal ENX con la fecha, el periodo de validez y si el resultado global de la evaluación es conforme o no conforme. Podría compartir ese resultado de la evaluación. Sin embargo, si comparte un resultado sin etiquetas TISAX, a la mayoría de destinatarios les parecerá que no ha superado la evaluación. En general, otros participantes de TISAX no aceptan los resultados de evaluación de un alcance

completamente personalizado.

Descripción: Como en el caso del alcance ampliado personalizado, si necesita un alcance completamente personalizado deberá redactar su propia descripción del alcance.

Nota importante:

Para recalcar lo raro que es el uso de alcances completamente personalizados: Hay un 98 % de posibilidades de que su proveedor de auditoría revierta su alcance completamente personalizado a un alcance estándar. Ningún participante ha elegido *nunca* un alcance completamente personalizado sin el asesoramiento de su proveedor de auditoría.

Una evaluación con alcance completamente personalizado no obtendrá etiquetas TISAX. Por tanto, solemos recomendar que no se elija el alcance completamente personalizado, sobre todo porque otros participantes no suelen aceptar los resultados de evaluaciones con alcance completamente personalizado.
No elija un alcance completamente personalizado si no tiene la confirmación explícita de que su socio aceptará el resultado y estará de acuerdo con su descripción del alcance.

7.9. Anexo: Gestión del ciclo de vida de los datos del participante

Las siguientes secciones describen qué tiene que hacer si se produce algún cambio en sus datos de participante.

7.9.1. Pérdida de acceso a los datos de participante (portal ENX)

Si no queda nadie en su empresa que tuviera acceso al portal ENX y por tanto a sus datos de participante, póngase en contacto con nosotros. Intentaremos ayudarle a recuperar el acceso a los datos de participante de su empresa.

7.9.2. Administración de contactos

Sus contactos de participante principal de la empresa y el resto de “contactos administrativos” con cuenta en el portal siempre podrán ir al portal ENX y:

- añadir nuevos contactos
- borrar contactos existentes
- cambiar la información de contacto de los contactos existentes

7.9.2.1. Cómo añadir un nuevo contacto

Para añadir un nuevo contacto, siga estos pasos:

1. Inicie sesión en el portal ENX.
2. Vaya a la barra de navegación principal y seleccione “MY TISAX” (“MI TISAX”).
3. En el menú desplegable, seleccione “ADMINISTRATORS” (“ADMINISTRADORES”).
4. Haga clic en el botón “Create new TISAX Administrator” (“Crear nuevo administrador TISAX”).
5. Introduzca los datos del contacto.
6. Haga clic en el botón “Save Contact” (“Guardar contacto”).
7. Vaya a la tabla y seleccione la fila con el contacto.
8. Vaya al final de la fila de la tabla del contacto y haga clic en el botón con la flecha hacia abajo .
9. Seleccione “Edit TISAX Administrator” (“Editar administrador TISAX”).
10. En la nueva ventana (“Edit TISAX Contact” (“Editar contacto TISAX”)), desplácese hacia abajo hasta la sección “ENX PORTAL ACCESS” (“ACCESO AL PORTAL ENX”).
11. Seleccione “Yes” (“Sí”).
12. En la sección que aparece “WEB ROLES” (“ROLES WEB”), haga clic en el botón “Add Role” (“Añadir rol”).
13. Seleccione el rol que quiere asignar (p. ej., “TISAX Administrator” (“Administrador TISAX”)).
14. Haga clic en el botón “Añadir rol”.
15. Haga clic en el botón “Guardar contacto”.

7.9.2.2. Cómo borrar un contacto existente

Para borrar un contacto existente, siga estos pasos:

1. Inicie sesión en el portal ENX.
2. Vaya a la barra de navegación principal y seleccione “MY TISAX” (“MI TISAX”).
3. En el menú desplegable, seleccione “ADMINISTRATORS” (“ADMINISTRADORES”).
4. Vaya a la tabla y seleccione la fila con el contacto.
5. Vaya al final de la fila de la tabla del contacto y haga clic en el botón con la flecha hacia abajo .
6. Seleccione “Delete TISAX Administrator” (“Borrar administrador TISAX”).
7. En la solicitud de confirmación que aparece, haga clic en el botón “Delete” (“Borrar”).

7.9.2.3. Cómo actualizar los datos de un contacto existente

Para actualizar los datos de un contacto existente, siga estos pasos:

1. Inicie sesión en el portal ENX.
2. Vaya a la barra de navegación principal y seleccione “MY TISAX” (“MI TISAX”).
3. En el menú desplegable, seleccione “ADMINISTRATORS” (“ADMINISTRADORES”).
4. Vaya a la tabla y seleccione la fila con el contacto.
5. Vaya al final de la fila de la tabla del contacto y haga clic en el botón con la flecha hacia abajo .
6. Seleccione “Edit TISAX Administrator” (“Editar administrador TISAX”).
7. Actualice los datos.
8. Haga clic en el botón “Save Contact” (“Guardar contacto”).

7.9.3. Administración de ubicaciones

Sus contactos de participante principal de la empresa y el resto de “contactos administrativos” con cuenta en el portal siempre podrán ir al portal ENX y solicitar:

- el cambio del nombre de la empresa
- el cambio de una ubicación (traslado)
- el cambio de un nombre de calle
- añadir una nueva ubicación

Describimos los pasos necesarios en las siguientes secciones.

Recuerde:

- En TISAX, la combinación de un nombre de empresa y una dirección define una “ubicación”.
- Cada ubicación tiene un “ID de ubicación” (los ID de ubicación siempre empiezan con una “L” y tienen una longitud de seis caracteres; ejemplo: L1L3XY).
- Si su empresa se traslada de su dirección actual a una nueva dirección, la ubicación anterior deja de ser una ubicación válida.

Nota importante:

Una vez que haya pulsado el botón “Guardar ubicación” en el portal ENX, ya no podrá cambiarla. Para las situaciones descritas a continuación, puede solicitar

el cambio correspondiente.

7.9.3.1. Cómo solicitar el cambio de nombre de su empresa

Su situación:	Su empresa ha cambiado de nombre.
Ejemplo:	El antiguo nombre de la empresa es “ACME Tires Corporation”. El nuevo nombre de la empresa es “ACME Corporation”.

Si quiere solicitar el cambio del nombre de la empresa, siga los siguientes pasos:

1. Inicie sesión en el portal ENX.
2. Vaya a la barra de navegación principal y seleccione “MY TISAX” (“MI TISAX”).
3. En el menú desplegable, seleccione “LOCATIONS” (“UBICACIONES”).
4. Vaya a la tabla y seleccione la fila con su ubicación.
5. Vaya al final de la fila de la tabla de la ubicación y haga clic en el botón con la flecha hacia abajo .
6. Seleccione “Request Change” (“Solicitar cambio”).
7. En la nueva ventana (“Request Change” (“Solicitar cambio”)), vaya al campo del formulario “Subject of the change” (“Asunto del cambio”), abra el menú desplegable y seleccione “Company Name” (“Nombre de la empresa”).
8. Rellene el resto del formulario
9. Envíe el formulario

Comprobaremos su solicitud, probablemente aceptaremos la petición de cambiar el nombre de la empresa, y le informaremos una vez listo.

7.9.3.2. Cómo solicitar un cambio de ubicación

Su situación:	Su empresa se ha trasladado a una nueva ubicación.
Ejemplo:	La antigua ubicación es “ACME Corporation, Bockenheimer Landstraße 97-99, 60325 Fráncfort, Alemania”. La nueva ubicación es “ACME Corporation, Behrenstraße 35, 10117 Berlín, Alemania”.

Nota importante:

Si una autoridad oficial ha cambiado el nombre de la calle de su ubicación, consulte la Sección 7.9.3.3, “Cómo solicitar el cambio de nombre de la calle” para obtener más información.

Si alguna de sus ubicaciones se traslada a una nueva dirección, siga estos pasos:

1. Cree una nueva ubicación:
   a. Inicie sesión en el portal ENX.
   b. Vaya a la barra de navegación principal y seleccione “MY TISAX” (🇪🇸 “MI TISAX”).
   c. En el menú desplegable, seleccione “Locations” (🇪🇸 “Ubicaciones”).
   d. Haga clic en el botón “Create TISAX Location” (🇪🇸 “Crear ubicación TISAX”).
   e. En la nueva ventana (“CREATE TISAX LOCATION” (🇪🇸 “CREAR UBICACIÓN TISAX”)), rellene el formulario con la información de la nueva ubicación.
   f. Haga clic en el botón “Save Location” (🇪🇸 “Guardar ubicación”).
2. Anote el “Location ID” (🇪🇸 “ID de ubicación”) de la ubicación recién creada. Encontrará el “ID de ubicación” en la primera columna de la tabla “MY LOCATIONS” (🇪🇸 “MIS UBICACIONES”). Su proveedor de auditoría necesita el "ID de ubicación" para actualizar el alcance de su evaluación en el portal ENX.
3. Informe del traslado a su proveedor de auditoría (facilitándole el “ID de ubicación” de la antigua ubicación, así como de la nueva).
   ¿Ha completado ya la evaluación?
   a. Si la respuesta es NO, usted ya no tendrá que hacer nada en relación con el cambio de ubicación.
   b. Si la respuesta es SÍ, deberá solicitar una “evaluación de ampliación del alcance” (🇬🇧 “scope extension assessment”) a su proveedor de auditoría. Para más información, consulte la Sección 7.10, “Anexo: Evaluación de la ampliación del alcance”.

Su proveedor de auditoría comprobará la solicitud y actualizará el alcance de su evaluación en el portal ENX.

Recuerde:

Un proveedor de auditoría solo puede actualizar su alcance de evaluación si usted ya ha encargado la evaluación a ese proveedor de auditoría.

7.9.3.3. Cómo solicitar el cambio de nombre de la calle

Su situación:	El nombre de la calle de su ubicación ha cambiado. Sin embargo, su empresa sigue estando en el mismo lugar físico.
Ejemplo:	La antigua ubicación es “ACME Corporation, Bockenheimer Landstraße 97-99, 60325 Fráncfort, Alemania”. La nueva ubicación es “ACME Corporation, Behrenstraße 97-99, 60325 Fráncfort, Alemania”.

Si una autoridad oficial ha cambiado el nombre de la calle de su ubicación, siga los siguientes pasos:

1. Inicie sesión en el portal ENX.
2. Vaya a la barra de navegación principal y seleccione “MY TISAX” (🇪🇸 “MI TISAX”).
3. En el menú desplegable, seleccione “Locations” (🇪🇸 “Ubicaciones”).
4. Vaya a la tabla y seleccione la fila con su ubicación.
5. Vaya al final de la fila de la tabla de la ubicación y haga clic en el botón con la flecha hacia abajo .
6. Seleccione “Request Change” (🇪🇸 “Solicitar cambio”).
7. En la nueva ventana (“Request Change” (🇪🇸 “Solicitar cambio”)), vaya al campo del formulario “Subject of the change” (🇪🇸 “Asunto del cambio”), abra el menú desplegable y seleccione “Address” (🇪🇸 “Dirección”).
8. Rellene el resto del formulario
9. Envíe el formulario

Comprobaremos su solicitud, probablemente aceptaremos la petición de cambiar el nombre de la calle, y le informaremos una vez listo.

Nota importante:

Estos pasos solo se aplican cuando su empresa sigue estando en el mismo lugar físico pero una autoridad oficial ha cambiado el nombre de la calle.
Si se ha trasladado a una nueva ubicación, consulte la Sección 7.9.3.2, “Cómo solicitar un cambio de ubicación” para obtener más información.

7.9.3.4. Cómo añadir una ubicación adicional

Si abre una ubicación adicional durante el periodo de validez de sus etiquetas TISAX existentes, puede solicitar una “evaluación de ampliación del alcance” (🇬🇧 “scope extension assessment”) a su proveedor de auditoría.

Para más información, consulte la Sección 7.10, “Anexo: Evaluación de la ampliación del alcance”.

7.10. Anexo: Evaluación de la ampliación del alcance

Además de los tipos de evaluación estándar descritos en Sección 5.4.3, “Tipos de evaluación TISAX”, existe otro tipo de evaluación especial: la “evaluación de la ampliación del alcance” (🇬🇧 “scope extension assessment”).

Puede ampliar un alcance de evaluación TISAX existente si desea añadir uno o varios:

- objetivos de evaluación o
- ubicaciones.

No puede seleccionar otro proveedor de auditoría para llevar a cabo la “evaluación de ampliación del alcance”. La evaluación es similar a los tipos de evaluación estándar. No obstante, su proveedor de auditoría seguramente procurará reutilizar los resultados aplicables de evaluaciones anteriores.

Una vez finalizada la evaluación de ampliación del alcance sin no conformidades, su proveedor de auditoría:

- actualizará el alcance de la evaluación en el portal ENX.
- emitirá el informe de evaluación de ampliación del alcance.

La evaluación de ampliación del alcance no alarga el periodo de validez original de sus etiquetas TISAX existentes.

Recuerde:

Si el motivo de la evaluación de la ampliación del alcance es un traslado o una ubicación adicional, deberá crear la nueva ubicación en el portal ENX.
Proporcione el “Extracto de ubicaciones” o al menos el “ID de ubicación” a su proveedor de auditoría.
Cada ubicación tiene un “ID de ubicación” (los ID de ubicación siempre empiezan con una “L” y tienen una longitud de seis caracteres; ejemplo: L1L3XY). Su proveedor de auditoría necesita el ID de ubicación para actualizar el resultado de la evaluación en el portal ENX.

7.11. Anexo: Gestión del ciclo de vida ISA

Un grupo de trabajo de ENX mantiene la ISA.

Esto le puede interesar:

- La VDA publica oficialmente nuevas versiones.
- El proveedor de auditoría utilizará la versión de la ISA válida en el momento en el que *encarga* su evaluación inicial
- De mutuo acuerdo, puede utilizar una versión de la ISA más reciente si se publica una entre su pedido y el comienzo de la evaluación inicial.
- Podrá encontrar la fecha de publicación de una determinada versión de la ISA en la hoja Excel “Portada”.
  - Ejemplo:

Versión: 5.0 | Revisión 4 | 2021-04-16

7.12. Anexo: Documentos útiles

Esta sección enumera algunos documentos que consideramos útiles.

- Libro blanco “Harmonization of classification levels” (Armonización de niveles de clasificación)

  “Este libro blanco describe la propuesta del grupo de trabajo sobre seguridad de la información para establecer un esquema centrado en el objetivo de protección de confidencialidad; es decir, que la información no se haga accesible a personas, organizaciones o procesos no autorizados. Los objetivos de protección como disponibilidad, integridad y fiabilidad no son objeto de este libro blanco.”

  Editor: Verband der Automobilindustrie e.V. (“Asociación alemana de la industria automotriz”)

  Idiomas disponibles: inglés, alemán

  https://www.vda.de/en/news/publications/publication/harmonization-of-classification-levels
  https://www.vda.de/de/aktuelles/publikationen/publication/whitepaper--harmonisierung-der-klassifizierungsstufen-

- Libro blanco “Information Security Risk Management” (Gestión de riesgos de seguridad de la información)

  “El objetivo de este libro blanco es informar a las empresas del sector del automóvil sobre la gestión de la seguridad de la información orientada al riesgo y permitirles establecer una gestión efectiva de los riesgos de seguridad de la información. Pretende asistir a las organizaciones durante la preparación o realización de una evaluación TISAX para cumplir los requisitos de la pregunta de control VDA ISA 1.4.1. Se deberá considerar como una recomendación de implementación, no como un requisito obligatorio.”

  Editor: Verband der Automobilindustrie e.V. (“Asociación alemana de la industria automotriz”)

  Idiomas disponibles: inglés, alemán

  https://www.vda.de/en/news/publications/publication/white-paper--information-security-risk-management-
  https://www.vda.de/de/aktuelles/publikationen/publication/whitepaper--risikomanagement-in-der-informationssicherheit-

7.13. Anexo: Gestión de reclamaciones

7.13.1. Motivos de reclamación

Nuestra gestión de reclamaciones distingue entre estas dos áreas:

1. ENX Association: la organización que rige TISAX
2. Proveedores de auditoría: las organizaciones que realizan las evaluaciones TISAX

7.13.1.1. Reclamaciones sobre ENX Association

Si tiene alguna reclamación sobre ENX Association, diríjase a nuestro “TISAX manager on duty” (responsable TISAX de guardia) (encontrará los datos de contacto más abajo)

7.13.1.2. Reclamaciones sobre los proveedores de auditoría

En primer lugar, debe intentar resolver el problema directamente con el auditor.

El siguiente paso debería ser la persona responsable de TISAX dentro del proveedor de auditoría.

A partir de ahí, su siguiente contacto sería la persona responsable de la gestión de calidad del proveedor de auditoría.

Si la cuestión sigue sin resolverse, diríjase a nuestro “TISAX manager on duty” (encontrará los datos de contacto más abajo).

Incluso hay opciones por encima del “TISAX manager on duty”. En casos así, hable con el director general de ENX Association.

La VDA no desempeña ningún rol en la gestión de reclamaciones.

Recuerde:

El proveedor de auditoría debe informarle sobre su derecho a reclamar durante la reunión inicial. Si no lo hace, esto ya sería motivo de reclamación.

7.13.1.3. Requisitos de las reclamaciones

Si desea implicarnos, necesitamos la siguiente información:

- ¿Quién realiza la reclamación?
  - Nombre de la empresa
  - ID de participante de TISAX
  - Contacto (nombre, dirección de correo electrónico, número de teléfono)

- ¿De qué evaluación se trata?
  - ID de evaluación
  - Si la evaluación aún no está registrada en el portal ENX: ID de alcance
- ¿Quién es el proveedor de auditoría?
  - Nombre de la empresa proveedora de auditoría
  - Nombre del auditor o auditores
- ¿Cuál es su reclamación?
  1. Reclamación general sobre la actuación del proveedor de auditoría
  2. Reclamación sobre el enfoque del auditor
  3. Reclamación sobre la evaluación en relación con el contenido
- Para las reclamaciones sobre la evaluación en relación con el contenido: ¿A qué hallazgo se opone?
  - Control (p. ej., 1.6.1 "¿En qué medida se procesan los eventos de seguridad de la información?")
  - Hallazgo (texto completo)
  - Oposición a:
    - Interpretación del control
    - Determinación en relación con el contenido (la evidencia disponible no se ha evaluado correctamente)
    - Evaluación de riesgo (no se ha considerado la pertinencia)
  - Razonamiento de por qué valora las cosas de modo diferente

7.13.2. Contacto para reclamaciones

Póngase en contacto con el “TISAX manager on duty”:

Envíe un mensaje de correo electrónico a:	tisax-complaints@enx.com
O llame al:	+49 69 9866927-79

Podrá localizarlo durante el horario de oficina habitual de Alemania (UTC+01:00).

Habla inglés y alemán.

8. Historial del documento

Versión: 2.7

- Cuatro idiomas añadidos (japonés, portugués de Brasil, italiano y coreano)
- Selector de idiomas para las versiones en HTML incorporado (en la esquina superior derecha)
- Diseño de las versiones en PDF mejorado
- Varias secciones actualizadas con los dos nuevos objetivos de evaluación de confidencialidad
- Sección “Lista de objetivos de evaluación” actualizada (descripción del objetivo de evaluación “Special data” corregida; nota sobre el cambio de etiquetas añadida)
- Corrección de erratas

Versión 2.6

- Nota general sobre los objetivos de evaluación y las etiquetas que hemos añadido en esta versión: En versiones anteriores, los objetivos de evaluación y las etiquetas tenían un “nombre oficial” largo y un “nombre corto” (Ejemplo: “Manejo de información con necesidad de protección alta” e “Info high”). Como la mayoría de la gente casi solo utilizaba el nombre corto, la forma corta es ahora el “nombre oficial”. El antiguo nombre largo ahora se denomina “Descripción”. Además, utilizamos *únicamente* el nombre oficial en inglés en el portal ENX y en todas las traducciones del Manual del participante de TISAX.
- Sección “Lista de objetivos de evaluación” actualizada con los dos objetivos de evaluación “High availability” y “Very favailability”, y “Figura 6. Objetivos de evaluación TISAX (representación en forma de tabla: nombre completo y abreviado)” eliminada.
- Sección “Objetivos de evaluación e ISA” actualizada para reflejar el hecho de que solo un subconjunto del catálogo de criterios “Seguridad de la información” se aplica a los dos objetivos de evaluación “High availability” y “Very high availability”
- Sección “Objetivos de evaluación y sus dependencias” eliminada
- Sección “Selección de los objetivos de evaluación” actualizada con los dos objetivos de evaluación “High availability” y “Very high availability”
- Sección “Necesidad de protección y niveles de evaluación” actualizada con los dos objetivos de evaluación “High availability” y “Very high availability”, y “Tabla 5. Asignación de los catálogos de criterios ISA y las necesidades de protección a los objetivos de evaluación TISAX” eliminada
- Sección “Catálogos de criterios” actualizada con los dos objetivos de evaluación “High availability” y “Very high availability”

- Sección “Requisitos” actualizada para reflejar el hecho de que solo un subconjunto del catálogo de criterios “Seguridad de la información” se aplica a los dos objetivos de evaluación “High availability” y “Very high availability”
- Sección “Jerarquía de las etiquetas TISAX” actualizada para reflejar el hecho de que ya solo existe una jerarquía en muy pocos casos y “Figura 36. Objetivos de evaluación TISAX y etiquetas TISAX (dependencias y jerarquía)” eliminada
- Sección “Anexo: Documentos útiles” actualizada para reflejar cambios en los enlaces
- Varias aclaraciones menores y pequeñas correcciones
- Corrección de erratas

Versión 2.5.1

- Corrección de enlaces rotos

Versión 2.5

- Sección “Administración de ubicaciones” añadida
- Sección “Anexo: Documentos útiles” actualizada para reflejar cambios en los enlaces

Versión 2.4

- Información imprecisa sobre la duración máxima del proceso de evaluación TISAX eliminada de la Sección 3.1, “Sinopsis”
- “Informe TISAX” cambiado a “informe de evaluación TISAX”
- Nota sobre las diferencias entre ISO 27001 y TISAX actualizada
- Sección “Descripción del alcance” actualizada; sección del alcance personalizado movida al anexo
- “Descripción del alcance estándar” actualizada a la versión 2.0
- Sección “Publicación y divulgación” actualizada con una nota sobre la divulgación del estado de la evaluación
- Sección “Necesidad de protección y niveles de evaluación” actualizada con contenido sobre el “nivel de evaluación 2.5”, el “método de evaluación a distancia asistido por vídeo”, las diferencias entre la AL 2 y la AL 3, y la comprobación de plausibilidad frente a la verificación
- Enlace al inicio del proceso de registro actualizado
- Sección “Cuenta en el portal” actualizada para reflejar el cambio en el proceso de invitación

- Enlaces de descarga al documento ISA cambiados (disponibles ahora en enx.com)
- Sección “Valoración de las ofertas” actualizada con una base para estimar los costes
- Sección “Reunión inicial” añadida (con contenido trasladado aquí desde la sección “La primera reunión inicial formal”)
- Sección “Acerca de la conformidad” actualizada con una nueva tabla sobre los cuatro tipos de hallazgo
- Sección “Evaluación inicial” actualizada con una nota relativa a las limitaciones de tiempo
- Sección “Informe de evaluación TISAX” actualizada con una nota relativa a un plan proactivo de acciones correctivas
- Sección “Preparación del plan de acciones correctivas” actualizada con los requisitos “hallazgo” y “causa raíz” y una nota relativa a las plantillas de planes de acciones correctivas
- Sección “Evaluación del plan de acciones correctivas” actualizada con una observación relativa al correo electrónico como único modo de comunicación
- Sección “Requisitos previos para una evaluación del plan de acciones correctivas” renombrada a “Motivos de una evaluación del plan de acciones correctivas” y dos motivos añadidos
- Sección “Etiquetas TISAX temporales” actualizada con ejemplos y aclaraciones sobre el periodo de validez
- Sección “Informe TISAX” renombrada a “Informe de evaluación TISAX”
- Sección “Renovación de las etiquetas TISAX” actualizada con una nota relativa a la reutilización de los registros de ubicación en el portal ENX
- Sección “Anexo: El razonamiento en contra de las “pre-evaluaciones” y los “análisis de deficiencias”” añadida
- Sección “Anexo: Alcances personalizados” añadida (“Alcance ampliado” y “Alcance reducido” sustituidos por “Alcance ampliado personalizado” y “Alcance completamente personalizado”)
- Sección “Anexo: Evaluación de la ampliación del alcance” actualizada con las razones y una nota relativa a cómo añadir registros de ubicación a la cuenta del participante en el portal ENX
- Sección “Anexo: Gestión del ciclo de vida ISA” actualizada para reflejar la situación actual
- Sección “Anexo: Documentos útiles” actualizada para reflejar cambios en los enlaces
- Sección “Anexo: Gestión de reclamaciones” añadida
- Ahora se puede hacer clic en los números de teléfono
- Varias aclaraciones menores y pequeñas correcciones
- Corrección de erratas

- Nota para los proveedores de auditoría TISAX: Esta actualización se basa en ID doc. ENX 612, versión 2.1

Versión 2.3

- Subtítulo reformulado
- Cambio de Word/PDF a HTML como formato primario del manual
- Más traducciones disponibles (chino y francés, véase el punto siguiente)
- Sección “El manual del participante de TISAX en otros idiomas y formatos” añadida
- Todos los enlaces a la página principal de ENX cambiados de "https://portal.enx.com" a "https://enx.com" (los enlaces antiguos siguen funcionando)
- “VDA ISA” se convierte en “ISA”
- Sección Sección 5.2, “Autoevaluación basada en la ISA” actualizada para reflejar los cambios introducidos con la versión 5 de la ISA
- Reordenación de las filas de todas las tablas con los objetivos de evaluación para que coincidan con el cambio de orden del catálogo de criterios en ISA 5
- Actualización de las figuras con los objetivos de evaluación para que coincidan con el cambio de orden de los catálogos de criterios en ISA 5
- Sección “Personalización del alcance” actualizada (figura 6, errata corregida, objetivos de evaluación actualizados)
- Sección “Tasa” actualizada con información sobre los pagos con tarjeta de crédito
- Sección “Diagrama del proceso de evaluación TISAX” actualizado (figura 34, referencia a Managed Service Provider eliminada)
- Sección “Anexo: Documentos útiles” actualizada (libro blanco “Information Security Risk Management” añadido)

Versión 2.2.1

- Corrección de erratas

Versión 2.2

- Problema con la impresión de la portada corregido
- Cambios en todos los enlaces a nuestra página principal y las descargas
- Ahora también hablamos italiano
- Sección “Alcance personalizado” ampliada

- Sección “Ubicaciones dentro del alcance” actualizada
- Objetivos de evaluación “Conexión con terceros” eliminados; figuras 7, 9 y 38 actualizadas; tablas 4, 5, 6 y 8 actualizadas
- Expresión “*con* el nivel de evaluación” cambiada a “*en* el nivel de evaluación”
- Referencia a la “lista de activación TISAX” en la sección “Necesidad de protección y niveles de evaluación” eliminada
  (ya no es aplicable)
- Sección “Objetivos de evaluación y sus propios proveedores»” añadida
- Sección “Contacto del participante” actualizada con información sobre las direcciones de correo electrónico genéricas y la forma de invitar a contactos para que puedan gestionar los datos de participante en el portal ENX
- Sección “Registro del alcance de la evaluación” actualizada con información sobre los cambios en el alcance de la evaluación
- Sección “Información de estado” actualizada (figura 12)
- Sección “Examine del resultado de la autoevaluación” actualizada con información sobre ayuda externa de terceros
- Sección “Cobertura” actualizada con un enlace a la matriz de cobertura de los proveedores de auditoría
- Sección “Solicitud de ofertas” actualizada
- Sección “Valoración de las ofertas” actualizada con información sobre las “evaluaciones previas”
- Sección “Renovación de las etiquetas TISAX” actualizada con información sobre la necesidad de registrar un nuevo alcance
- Varias subsecciones de la sección “Intercambio (paso 3)” actualizadas para reflejar cambios en la interfaz en el portal ENX
- Sección “Compartir el resultado de la evaluación con un participante concreto” actualizada con recomendaciones sobre el nivel de divulgación y una nota sobre el procesamiento automático de los resultados de evaluación compartidos
- Sección “Compartir el resultado de la evaluación fuera de TISAX” añadida
- Sección “Gestión del ciclo de vida ISA” añadida
- Sección “Anexo: Estado del alcance de la evaluación” actualizada (nuevo estado “Pendiente del pedido”, estado “Pendiente de aprobación” renombrado a “Pendiente de aprobación ENX”, estado “Aprobado” renombrado a “Pendiente de pago”, figura 40)
- Sección “Anexo: Ejemplo de mensaje de correo electrónico de confirmación” actualizada
- Sección “Anexo: Ejemplo de TISAX Scope Excerpt” actualizada
- Sección “Anexo: Estado de la evaluación” actualizada (nuevo estado “Evaluación inicial en

curso”, estado “A la espera de la evaluación de seguimiento” renombrado a “A la espera del seguimiento”, figura 41)

- Sección “Anexo: Evaluaciones antiguas de Volkswagen” (y sus referencias) eliminada (ya no es relevante)

Versión 2.1.2

- Límite formal de la “distancia” entre “su puntuación final” y el “resultado máximo” corregido del 25 % al 30 %

Versión 2.1.1

- Corrección de erratas

Versión 2.1

- Sección “Managed Service Providers” eliminada
- Nuevos objetivos de evaluación TISAX / etiquetas (etiquetas de protección de datos según el RGPD; cuatro etiquetas de prototipos en lugar de dos; cambio de nombre: necesidad de protección en lugar de niveles de protección; consejos para la selección actualizados)
- Actualizaciones debidas a cambios en la ISA (versión 4.0 a 4.1)
- Referencia al nuevo documento “TISAX Simplified Group Assessment” (apéndice a este manual)
- Sugerencias para la asignación de nombres de ubicación y nombres de alcance añadidas
- “Tasa de registro” renombrada a “tasa”
- Recomendación sobre sustitutos para los contactos añadida
- Selección del modelo de cargo eliminada

Volver al inicio.

[1] Tal vez quiera llevar a cabo el proceso TISAX como medida preventiva. Algunas empresas lo hacen para estar mejor preparadas. Disponer de una evaluación TISAX puede traducirse en una fase de contratación más corta y puede darle la ventaja sobre otros competidores que todavía no cuenten con la evaluación TISAX.

[2] Las “etiquetas TISAX” son un concepto para resumir el resultado de la evaluación y son el producto del proceso TISAX.

Consulte la Sección 5.4.14, “Etiquetas TISAX” para más información.

[3] La mayoría de los pasos de registro solo son necesarios una vez cuando empieza como participante de TISAX. Cuando renueva el resultado de la evaluación, solo tiene que actualizar y confirmar los datos de registro.

[4] Publicaremos los cambios de nuestras Condiciones generales en el portal ENX y notificaremos a los contactos registrados.

[5] Esto también se aplica al resto de acuerdos adicionales (p. ej., códigos de conducta).

[6] Recuerde que actualmente no se informa automáticamente a su socio sobre nuevos permisos. Quizá quiera notificarle a su socio que los resultados de la evaluación están disponibles.

[7] Si quiere figurar en esa lista, póngase en contacto con nosotros.

[8] Una evidencia es cualquier cosa que demuestre su afirmación de cumplir cierto requisito. Las evidencias suelen ser documentos. Sin duda, usted usará documentación interna como evidencia.

[9] Las entrevistas para las evaluaciones del nivel de evaluación 2 se suelen celebrar por videoconferencia. Si usted lo solicita, se pueden realizar en persona

[10] El mínimo teórico para las evaluaciones en grupo simplificadas es de tres ubicaciones.

[11] Si ya sabe que tendrá que mejorar el sistema de gestión de la seguridad de la información, el mínimo recomendado es de doce ubicaciones.

[12] Para evitar una posible confusión entre números y letras (como el 8 y la B), determinadas letras no se permiten en el ID de participante. No obstante, algunos ID de participante antiguos pueden contener la letra “G”.

[13] La ISA también se refiere a los catálogos de criterios con el término “módulos”.

[14] Encontrará esta función de Excel en la cinta de opciones “Datos”, sección “Esquema”.

[15] ¿Su empresa tiene otros proveedores de auditoría para evaluaciones similares (como ISO 27001) que están interesados en realizar también evaluaciones TISAX? Comparta este manual y dígales que se pongan en contacto con nosotros para averiguar qué necesitan para convertirse en proveedor de auditoría TISAX

[16] Los proveedores de auditoría que no estén incluidos en nuestro listado no están autorizados a llevar a cabo evaluaciones TISAX.

[17] Si finaliza el proceso de evaluación, no recibirá etiquetas TISAX.

[18] En realidad, existe un cuarto tipo: la “evaluación de la ampliación del alcance”. Como se trata de un caso especial, se describe en detalle en el anexo: Sección 7.10, “Anexo: Evaluación de la ampliación del alcance”.

[19] La reunión *inicial* formal se describirá en detalle para la evaluación inicial. Para el resto de evaluaciones TISAX, el proveedor de auditoría programará y definirá estas reuniones.

[20] Algunos proveedores de auditoría puede que usen el término “reunión inicial” como sinónimo de “reunión inicial formal”.

[21] La reunión *final* formal se describirá en detalle para la evaluación inicial. Para el resto de evaluaciones TISAX, el proveedor de auditoría programará y definirá estas reuniones.

[22] Si no se puede resolver una disputa, podrá elevarla a una instancia superior. Para más información, consulte la Sección 7.13, “Anexo: Gestión de reclamaciones”.

[23] Para más información sobre los métodos de auditoría y la intensidad, consulte la Sección 4.3.3.5, “Necesidad de protección y niveles de evaluación”.

[24] Si no se puede resolver una disputa, podrá elevarla a una instancia superior. Póngase en contacto con nosotros para más información.

[25] Recuerde que su resultado global de la evaluación puede seguir siendo “no conforme con una desviación importante” incluso si ha definido acciones correctivas adecuadas. Ese es el caso si sus medidas no tienen un efecto inmediato.

[26] Lógicamente, esto solo se aplica si en la evaluación inicial se identificaron no conformidades. No necesita una evaluación de seguimiento para las evaluaciones iniciales con un resultado de “conforme”.

[27] En teoría, puede ser nueve meses tras la conclusión de la evaluación inicial.

[28] En realidad, existe un cuarto tipo: el “informe de evaluación de ampliación del alcance”. Como se trata de un caso especial, se describe en detalle en: Sección 7.10, “Anexo: Evaluación de la ampliación del alcance”.

[29] El “informe de evaluación TISAX” se basa en una plantilla que todos los proveedores de auditoría TISAX están obligados a utilizar.

[30] La palabra “renovar” puede malinterpretarse. Para mantener una etiqueta TISAX durante más de tres años, debe volver a pasar el proceso TISAX, empezando por el registro de un nuevo alcance de evaluación.

[31] No mantenemos una lista “pública en TISAX” con los ID de participante. De esta forma se evita compartir accidentalmente los resultados con empresas de nombre similar o por otros “errores humanos”. Por ese motivo, siempre deberá contactar con su socio para obtener el ID de participante.

[32] Su socio ha de iniciar sesión en el portal y buscar activamente el resultado de la evaluación que usted ha compartido. Este no recibirá ninguna notificación automática sobre nuevos resultados de evaluación.

[33] La norma está definida en las “Condiciones generales de participación en TISAX” (https://enx.com/tisaxgtcen.pdf).

[34] Durante el estado del alcance de la evaluación “Pendiente de pago” o “Registrado”, la “Información relativa a la evaluación” incluye la o las ubicaciones del alcance de la evaluación, el estado del alcance de la evaluación y el o los objetivos de evaluación. No incluye los resultados de la evaluación ni etiquetas TISAX.

[35] Las “etiquetas TISAX” son un concepto para resumir el resultado de la evaluación y son el producto del proceso TISAX. Consulte la Sección 5.4.14, “Etiquetas TISAX” para más información.