Universidad de la Ciudad de Aguascalientes

ISO/IEC 27701 - Sistema de Gestión de

Privacidad de la Información

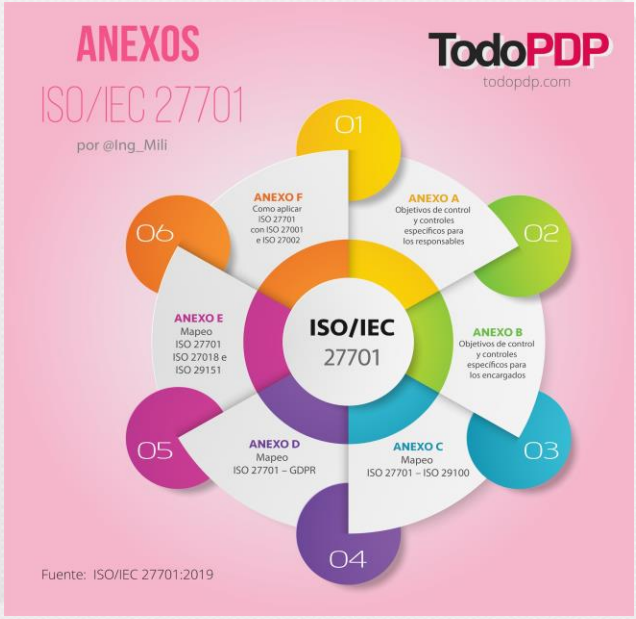
Marco Antonio Rodríguez Rangel

Mentes que transforman el mundo

Introducción

La norma ISO/IEC 27701, publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrónica Internacional (IEC), establece los requerimientos para que las empresas implementen un Sistema de Gestión de Privacidad de la Información (SGPI). También se le conoce como Sistema de Gestión de la Información sobre la Privacidad (PIMS por sus siglas en inglés).

Dicho de otra forma, esta norma funciona como una guía para los responsables del tratamiento de datos personales dentro de la empresa, de manera que puedan crear, implementar y optimizar un SGPI que les permita resguardar la privacidad digital de la información.



¿Quién debería de utilizar la norma ISO/IEC 2701?

Deben utilizarla las siguientes organizaciones:

Organizaciones que gestionan información personal (PII): Empresas y entidades que recogen, procesan, almacenan o transmiten datos personales.

Responsables del tratamiento de datos (Data Controllers): Organizaciones que deciden los propósitos y medios para procesar datos personales, es decir, aquellas que tienen el control sobre cómo se manejan los datos personales de los usuarios.

Encargados del tratamiento de datos (Data Processors): Empresas que procesan datos personales en nombre de los responsables de los datos. Esto incluye proveedores de servicios en la nube, empresas de análisis de datos, y otras organizaciones que procesan datos en nombre de terceros.

Organizaciones que buscan cumplir con regulaciones de privacidad: Aquellas que necesitan cumplir con leyes de protección de datos como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, o la Ley de Privacidad del Consumidor de California (CCPA) en los Estados Unidos, entre otras.

Empresas que desean mejorar la confianza con sus clientes: Implementar esta norma puede mejorar la confianza de los usuarios y clientes, al demostrar un compromiso con la privacidad y la protección de datos.

¿Quién debería de utilizar la norma ISO/IEC 2701?

Objetivo

La norma ISO/IEC 27701 tiene como objetivo principal reforzar la gestión de la privacidad de la información personal (PII) dentro de una organización; Además de tener los siguientes objetivos igual de importantes:

Proteger la Información Personal Identificable (PII)

Facilitar el cumplimiento normativo

Mejorar la confianza de los interesados.

Definir roles y responsabilidades claras

Minimizar riesgos relacionados con la privacidad

Mejorar la gestión de incidentes relacionados con la privacidad

Universidad de la Ciudad de Aguascalientes

Principales normativas - directrices

Mentes que transforman el mundo

Roles y responsabilidades: Responsables y Encargados del tratamiento

La norma establece dos roles fundamentales:

Responsable del tratamiento: Entidad que determina los fines y medios del tratamiento de datos personales.

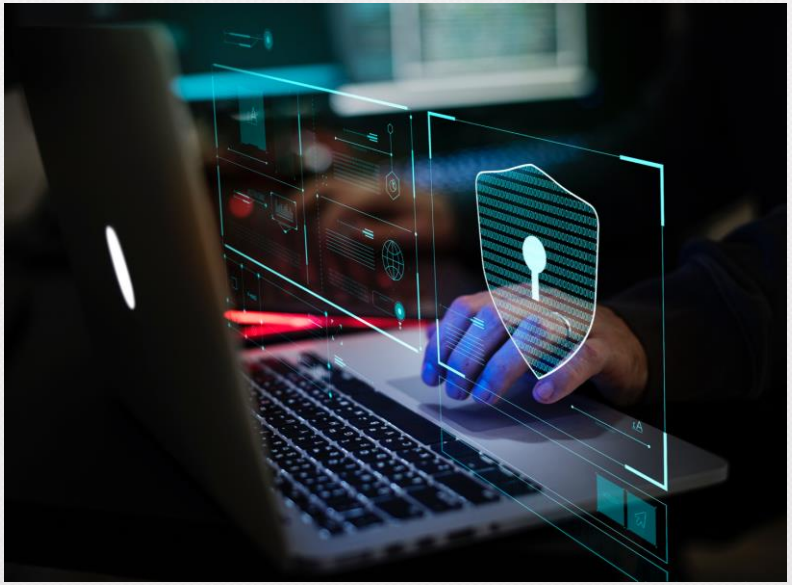
Encargado del tratamiento: Entidad que trata los datos personales en nombre del responsable del tratamiento.

Requisitos específicos de seguridad para la privacidad

ISO/IEC 27701 establece controles de seguridad específicos para la protección de la información personal (PII - Personally Identifiable Information), como:

Evaluación de riesgos relacionados con la privacidad.

Medidas de seguridad técnicas y organizativas para proteger la información personal.

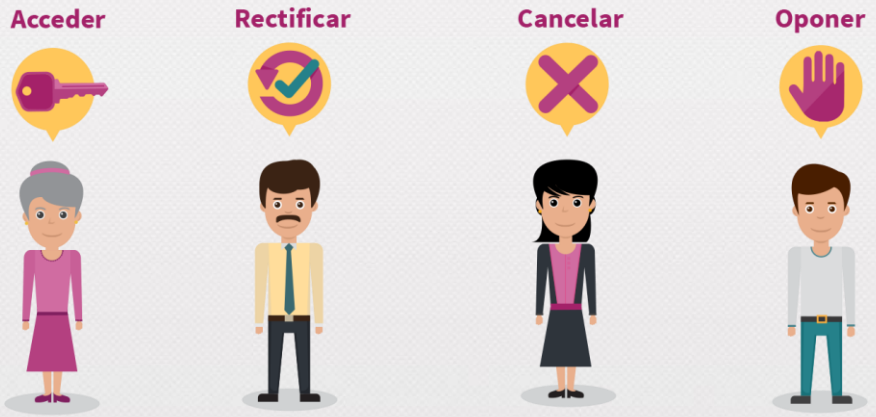


Derechos del titular de los datos

La norma requiere que las organizaciones implementen procedimientos para:

Responder a las solicitudes de los titulares de los datos en cuanto a acceso, rectificación, borrado o limitación del tratamiento.

Garantizar la transparencia sobre el tratamiento de los datos personales.



Consentimiento y legitimidad del tratamiento

ISO/IEC 27701 exige que las organizaciones aseguren que el tratamiento de datos personales sea legítimo y que, cuando sea necesario, se obtenga el consentimiento de los titulares de los datos de manera adecuada y clara.

Transparencia y políticas de privacidad

Es fundamental que las organizaciones implementen políticas claras que informen a los titulares de los datos sobre:

Qué datos se recopilan.

Por qué se recopilan.

Cómo se procesan, almacenan y comparten.

Derechos de los titulares y medios para ejercerlos.

Transferencia de datos internacionales

Se deben establecer procedimientos para asegurar la protección de datos transferidos internacionalmente, cumpliendo con las regulaciones aplicables (por ejemplo, GDPR para las empresas que operan en la UE).

Gestión de incidentes de seguridad relacionados con la privacidad

Las organizaciones deben tener un sistema para:

Detectar, notificar y gestionar incidentes que involucren la violación de datos personales.

Implementar medidas correctivas y preventivas.

Evaluaciones de impacto de la privacidad (PIA)

ISO/IEC 27701 promueve la realización de evaluaciones de impacto sobre la privacidad, con el fin de identificar y mitigar los riesgos asociados con el tratamiento de datos personales.

Mantenimiento y mejora continua

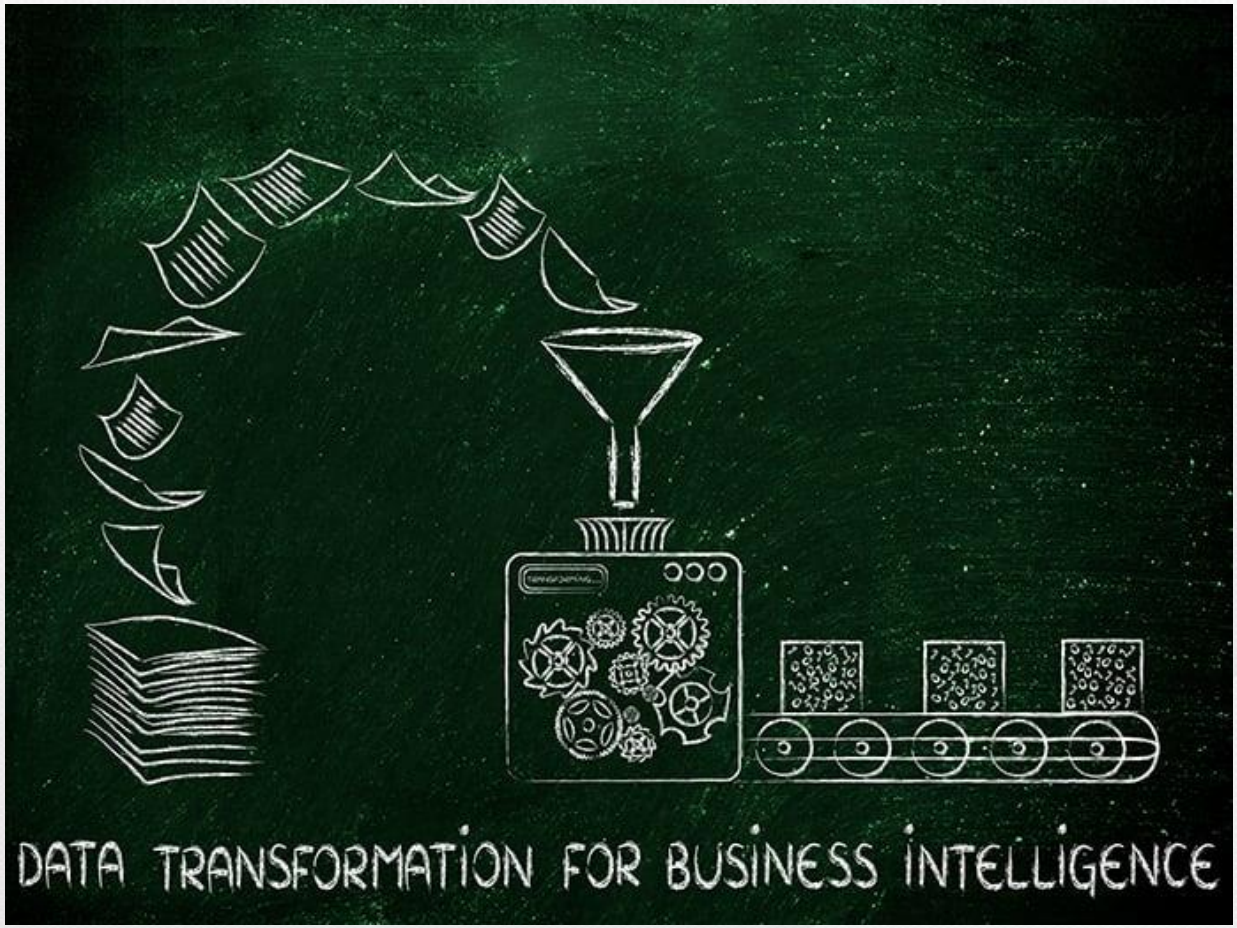
La norma enfatiza la importancia de monitorear y revisar regularmente el sistema de gestión de la privacidad para asegurar su efectividad y cumplimiento con las leyes y regulaciones de protección de datos, promoviendo la mejora continua.

Cumplimiento normativo y legal

ISO/IEC 27701 también especifica que las organizaciones deben estar al tanto y cumplir con las regulaciones legales aplicables sobre protección de datos, como el Reglamento General de Protección de Datos (GDPR) en la UE, y otras normativas locales o sectoriales.

Confidencialidad y minimización de datos

Se promueve la implementación de principios como la minimización de datos (recopilar solo los datos necesarios) y la confidencialidad en el manejo de la información personal.



Universidad de la Ciudad de Aguascalientes

Impacto global y adopción

Mentes que transforman el mundo

Impacto Global y Adopción

Cumplimiento Normativo

- Facilitación del Cumplimiento: La ISO/IEC 27701 proporciona un marco que ayuda a las organizaciones a cumplir con regulaciones como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

Mejora de la Gestión de la Privacidad

- Gestión Integral: La norma adopta un enfoque integral para la gestión de la privacidad de la información, permitiendo a las organizaciones definir roles y responsabilidades claras en relación con la protección de datos personales.

Aumento de la Confianza

- Confianza del Cliente: Al implementar la ISO/IEC 27701, las organizaciones pueden demostrar su compromiso con la privacidad, lo que contribuye a aumentar la confianza de los clientes y partes interesadas en su capacidad para manejar información personal de manera segura.

Diversidad de Sectores

- Aplicabilidad Universal: La ISO/IEC 27701 es aplicable a todo tipo de organizaciones, independientemente de su tamaño o sector, lo que ha facilitado su adopción en diversas industrias, desde el sector público hasta el privado y organizaciones sin fines de lucro.

Integración con Otros Sistemas de Gestión

- Extensión de ISO 27001: La norma se basa en la ISO/IEC 27001 y se puede implementar junto con esta, lo que permite a las organizaciones que ya tienen un Sistema de Gestión de Seguridad de la Información (SGSI) ampliar su enfoque para incluir la privacidad de la información.

Desafíos en la Adopción

- Difusión Limitada: A pesar de sus beneficios, la adopción de la ISO/IEC 27701 ha sido más lenta de lo esperado. Muchas organizaciones aún no han implementado este estándar, lo que puede ser un obstáculo en un entorno digital donde los riesgos de seguridad de la información están en aumento.

Certificación y Reconocimiento

- Reconocimiento Global: La certificación ISO/IEC 27701 es reconocida internacionalmente, lo que otorga a las organizaciones una ventaja competitiva al demostrar su compromiso con la privacidad y la protección de datos.

Universidad de la Ciudad de Aguascalientes

Desafíos

Mentes que transforman el mundo

La implementación de la norma ISO/IEC 27701 puede presentar varios desafíos para las organizaciones. A continuación se detallan algunos de los más comunes:

Falta de Conocimiento y Capacitación:

Comprensión de la Norma: Muchas organizaciones carecen del conocimiento necesario sobre los requisitos específicos de la ISO/IEC 27701 y cómo se relaciona con sus sistemas existentes, especialmente si ya han implementado la ISO/IEC 27001.

Capacitación del Personal: La falta de formación adecuada para el personal en temas de gestión de privacidad y protección de datos puede dificultar la implementación efectiva de la norma.

Integración con Sistemas Existentes

Compatibilidad: Integrar la ISO/IEC 27701 con sistemas de gestión de seguridad de la información existentes (como la ISO/IEC 27001) puede ser complicado. Es esencial que las organizaciones adapten sus procesos y políticas para cumplir con ambos estándares.

Recursos Adicionales: La implementación de un Sistema de Gestión de Privacidad de la Información (SGPI) puede requerir recursos adicionales, tanto humanos como financieros, lo que puede ser un obstáculo, especialmente para las pequeñas y medianas empresas.

Gestión del Cambio

Resistencia Interna: Puede haber resistencia al cambio por parte del personal, especialmente si no se comprende completamente la importancia de la privacidad de los datos y cómo afecta a la organización.

Cultura Organizacional: Cambiar la cultura organizacional para priorizar la privacidad y la protección de datos puede ser un desafío significativo, especialmente en empresas donde la seguridad de la información no ha sido una prioridad.

Recursos Financieros

Costos de Implementación: Los costos asociados con la implementación de la norma, que incluyen formación, auditorías y posibles actualizaciones de sistemas, pueden ser significativos y representar un desafío para muchas organizaciones.

Conclusión

La ISO/IEC 27701 proporciona un marco robusto para la gestión de la privacidad de la información, ayudando a las organizaciones a proteger la información personal y a cumplir con las regulaciones pertinentes, promoviendo así un entorno de confianza y seguridad en la gestión de datos.

Aunque la implementación puede presentar desafíos, los beneficios en términos de seguridad, cumplimiento legal y confianza del cliente justifican el esfuerzo.

Referencias

https://www.piranirisk.com/es/blog/conoce-iso-27701-gestion-privacidad-de-informacion

https://www.nqa.com/es-mx/certification/standards/iso-27701

https://www.pmg-ssi.com/2020/06/en-que-consiste-iso-iec-27701/

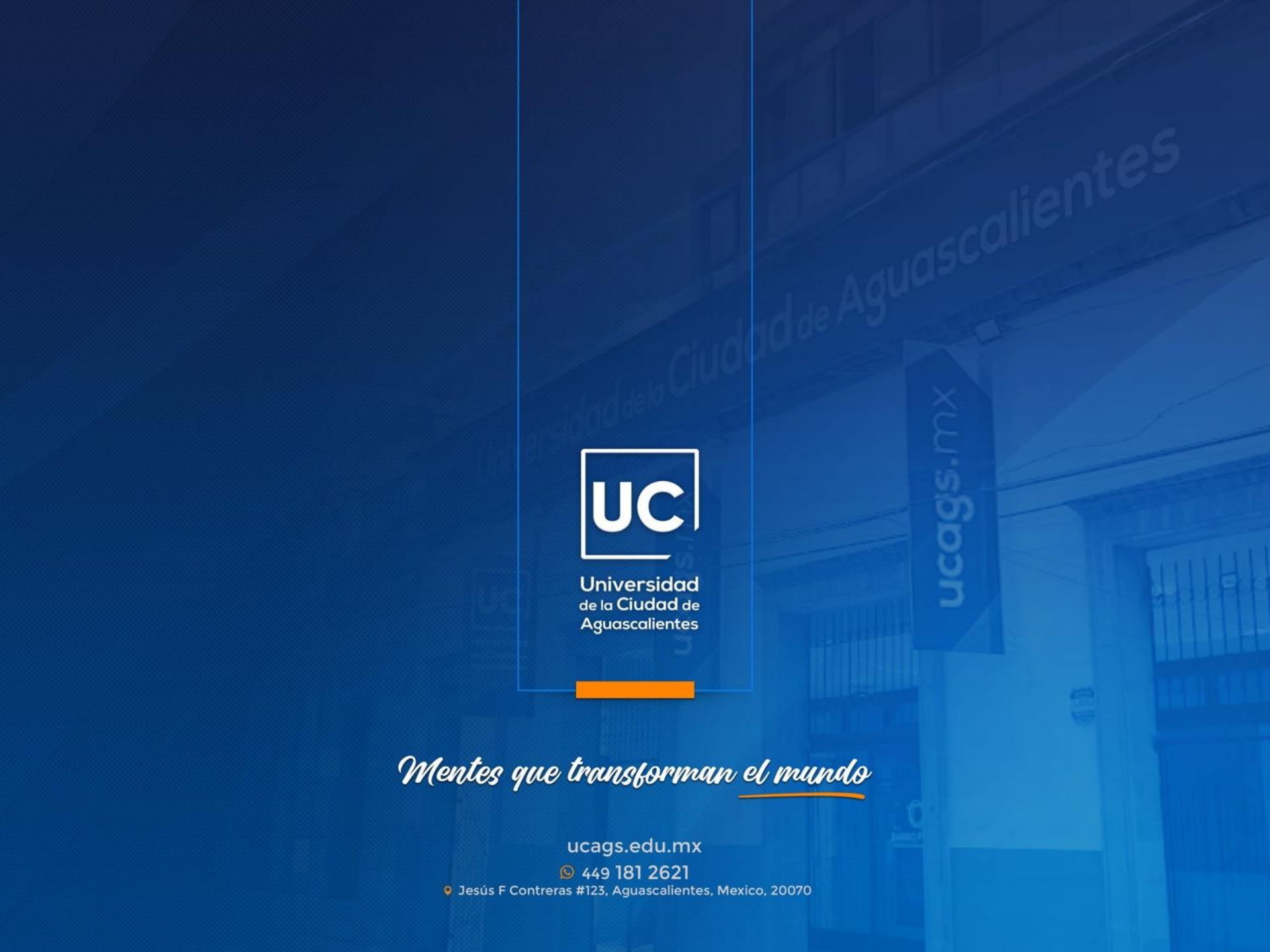
https://www.globalsuitesolutions.com/es/webinar-errores-comunes-proyecto-iso-27001/

https://www.pmg-ssi.com/2014/11/iso-27001-desafios-para-las-organizaciones-en-seguridad/

https://www.bsigroup.com/es-MX/gestion-de-la-privacidad-de-la-informacion-iso-27701/

https://www.net-learning.com.ar/blog/buenas-practicas-en-la-proteccion-de-datos-personales-en-plataformas-de-e-learning.html

https://www.deltaprotect.com/blog/norma-iso-27701-que-es


Universidad
de la Ciudad de
Aguascalientes
Mentes que transforman el mundo
ucags.edu.mx
449 181 2621
Jesús F Contreras #123, Aguascalientes, Mexico, 20070