Convergence
SERVICES

ISOs y Certificaciones

Importancia de las certificaciones empresariales

Convergence
SERVICES

Contar con las certificaciones internacionales en tu empresa conlleva diferentes beneficios, dentro de los principales es la satisfacción del cliente, esto como estrategia de negocio.

Al ser una empresa certificada transmite seguridad a los clientes, ya que brinda de manera adicional a su foco principal “el producto/servicio” y orienta los objetivos al cliente para operar en la línea correcta con base a los estándares internacionales y sobre con los que se miden todas las empresas que son altamente competitivas, abriendo a la empresa a mayores oportunidades.

Con estos antecedentes se entenderá al cliente y lo guiaremos para lograr su satisfacción total, a través de las certificaciones, nuestro cliente será capaz de agregar valor relacionado a la calidad, relación, procesos, rendimiento, precio y beneficios.

Contar con las certificaciones adecuadas refleja que la organización está abierta a nuevas oportunidades y alianzas, así como el cuidado por la información de los clientes, posicionando al mismo nivel que los grandes competidores.

Por último, a corto plazo los beneficios de una certificación y la correcta asesoría se traducen en mejoras en los procesos internos de la organización. Disminuye errores en la operación como el retrabajo, además de aumentar la calidad y la conformidad de los productos. Los ahorros impactan en la posibilidad de invertir en el desarrollo de nuevos y mejores productos, en reformas y actualizaciones de instalaciones y equipo o en la adquisición de nuevas tecnologías.

Somos consultores con experiencia con la cual acompañamos a nuestros clientes antes y durante el proceso de certificación de su empresa, así garantizamos la certificación y poder obtener los beneficios previamente mencionados.

Las ISOs y certificaciones en las que brindamos el servicio de consultoría y acompañamiento, son los siguientes:

Certificación ISO 27001

Certificación ISO 22301

Certificación SOC

Certificación PCI

Certificación ISO 27001

(SGSI: Sistema de Gestión de Seguridad de la Información)

Un Sistema de Gestión de Seguridad de la Información (SGSI) permite a las organizaciones conocer, gestionar y minimizar los riesgos relacionados con la seguridad de la información de una forma sistemática y eficiente. La adecuada implantación y certificación de este esquema ofrece una garantía de confidencialidad, integridad y disponibilidad de los datos almacenados.
La certificación de un Sistema de Gestión de Seguridad de la Información genera confianza a los clientes y mejora la eficiencia de la empresa.

Beneficios:

- Minimizar los riesgos inherentes a la seguridad de la información (pérdida de datos, robo, corrupción, etc.)
- Garantizar el cumplimiento legal
- Generar confianza en los clientes asegurando la buena gestión de los datos confiados a su organización (gracias a su reconocimiento internacional)
- Proteger la información y garantizar su seguridad
- Identificar los riesgos derivados del almacenamiento de información
- Facilitar la comprensión del estándar y su integración con otros sistemas de gestión

La certificación ISO 27001 va dirigida a cualquier empresa, independientemente de su tamaño o de su actividad, puede certificar su SGSI de acuerdo con ISO 27001:2022. Actualmente destaca la presencia de este estándar en las empresas dedicadas a servicios de tecnología de la información, así como aseguradoras, minoristas, compañías del sector del transporte, gobiernos, etc

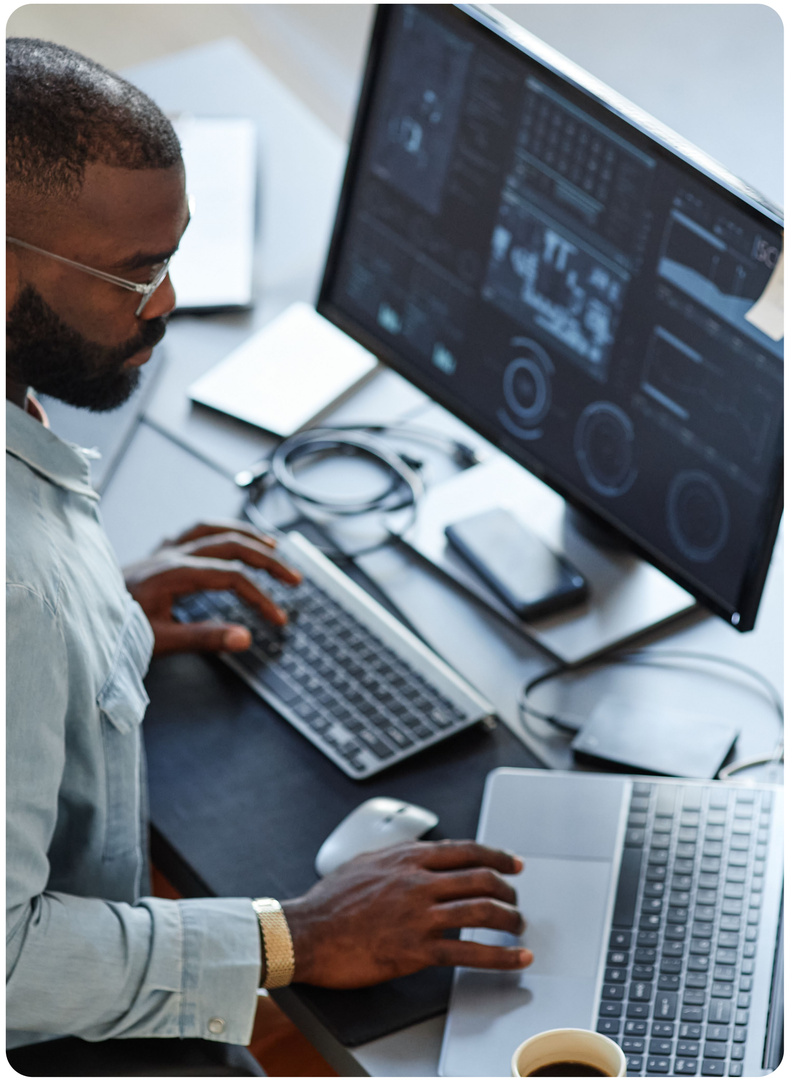
Certificación ISO 22301
(SGCN: Gestión de la Continuidad de Negocio)

En caso de emergencia, las empresas deben tener la capacidad de mitigar los daños y seguir operando. La ISO 22301 es la norma internacional para la Gestión de la Continuidad de Negocio (SGCN). Publicado por la Organización Internacional de Normalización, la ISO 22301 está diseñada para ayudar a las organizaciones a prevenir, preparar, responder y recuperarse de incidentes inesperados. Para ello, la norma proporciona un marco práctico con el fin de establecer y gestionar un sistema de gestión de continuidad de negocio eficaz. La ISO 22301 tiene como objetivo proteger a la organización de una amplia gama de posibles amenazas e interrupciones.

Esta norma puede ser adecuada para su organización si necesita demostrar a las partes interesadas que su organización puede superar rápidamente cualquier interrupción operativa con el fin de proporcionar un servicio continuo y eficaz.

Beneficios:

- Tener la capacidad de resistir los efectos de un incidente (resiliencia) así como prevenir o evitar los posibles escenarios originados por una situación de crisis
- Gestionar la interrupción de sus actividades minimizando las consecuencias económicas, de imagen o de responsabilidad civil derivadas de la misma
- Generar confianza en los clientes asegurando la buena gestión de los datos confiados a su organización (gracias a su reconocimiento internacional)
- Reducir los costes asociados a la interrupción
- Evitar penalizaciones por incumplimiento de contratos como proveedor de productos o servicios
- Disponer de una metodología estructurada para reanudar sus actividades después de una interrupción



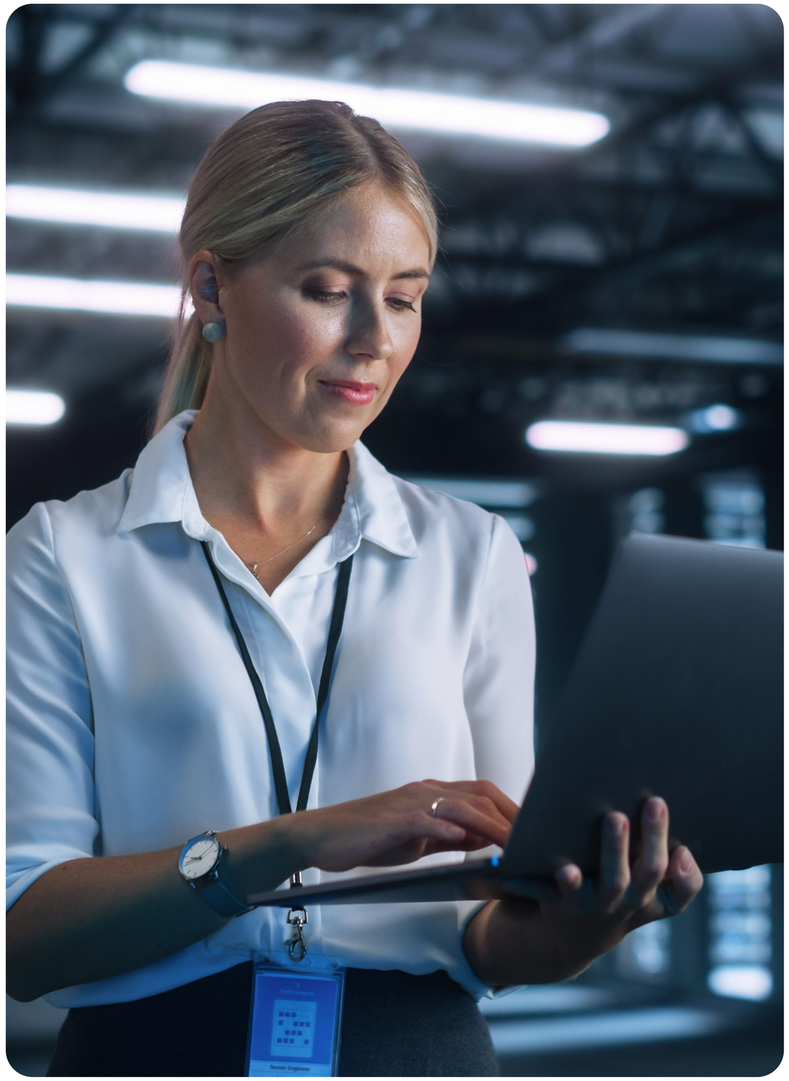
Certificación SOC
(Controles de organización de servicios)

Los controles del sistema y de la organización (SOC) para las empresas de servicios, son informes de control interno creados por el Instituto Estadounidense de Contadores Públicos Certificados (AICPA) y estuvieron incluidos dentro de los criterios del servicio de confianza del AICPA, que facilitan la auditoría y los informes sobre los controles que utiliza una organización de servicios para proteger la información, lo cual ayuda a los clientes a que puedan evaluar y abordar el riesgo asociado a un servicio subcontratado.

Una certificación de controles de organización de servicios (SOC 2) es una auditoría independiente de las prácticas de seguridad de las empresas. Cuando una empresa supera una auditoría SOC 2, está mostrando tanto a clientes potenciales como a los existentes, que tiene prácticas sólidas de ciberseguridad.

Los informes de SOC 2 captan la seguridad, la disponibilidad, la integridad del procesamiento, la confidencialidad y la privacidad de los datos.

1. **Seguridad:** protección de datos y seguridad del sistema contra el acceso no autorizado y la exposición de datos. La seguridad también incluye la protección frente a daños en el sistema que podrían provocar la pérdida de la disponibilidad, integridad y confidencialidad de los datos
2. **Disponibilidad:** fiabilidad de los sistemas que se necesita para que la entidad pueda seguir trabajando normalmente
3. **Integridad del procesamiento:** el procesamiento del sistema debe ser total, válido, preciso, en el momento oportuno y estar autorizado
4. **Confidencialidad:** los datos clasificados como "confidenciales" deben protegerse para que se puedan cumplir los objetivos de la entidad
5. **Privacidad:** la información debe recopilarse, utilizarse, conservarse, divulgarse y desecharse para que se puedan cumplir los objetivos de la entidad en materia de privacidad de datos



Certificación PCI
(Estándar de Seguridad de Datos para Tarjeta de Pago)

En un mundo cada vez más digital e interconectado, proteger la información confidencial de los clientes y garantizar la seguridad de las transacciones se ha convertido en algo esencial. Una de las principales formas que tienen las empresas de demostrar su compromiso con la seguridad de los datos es a través de certificados de seguridad como PCI DSS.

Específicamente para las empresas que procesan transacciones con tarjetas de pago, el PCI DSS (Payment Card Industry Data Security Standard) es una norma de seguridad establecida por las principales compañías de tarjetas de pago, como Visa, Mastercard, American Express y otras.

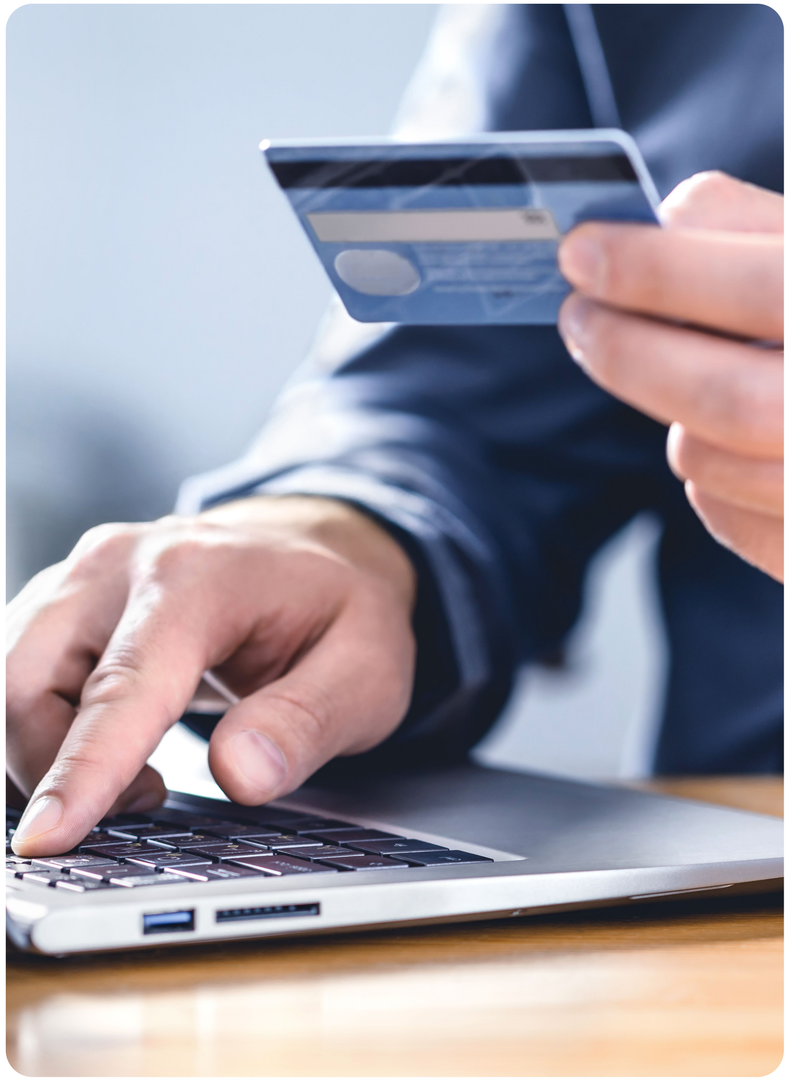
El PCI DSS es un conjunto de requisitos de seguridad cuyo objetivo es proteger los datos sensibles de los clientes durante las transacciones con tarjetas de pago de punta a punta, es decir, abarcando todos los aspectos del almacenamiento, procesamiento y transmisión de los datos de las tarjetas.

Siguiendo las directrices de PCI DSS, las empresas pueden establecer un entorno seguro para el procesamiento de transacciones y, como resultado, minimizar las posibilidades de que se produzcan brechas de seguridad y proteger la confianza de los clientes.

Al obtener la certificación PCI DSS, las empresas demuestran su compromiso con la seguridad de los datos y refuerzan su postura de seguridad garantizando transacciones seguras y fiables.

Las organizaciones deben cumplir una serie de requisitos establecidos por el consejo de seguridad de la PCI. Estos son:

- Construir y mantener una infraestructura de red segura
- Evaluación y análisis de riesgos para proteger los datos personales de los titulares de tarjetas
- Mantener una política de seguridad global que abarque todos los aspectos del procesamiento de pagos con tarjeta
- Aplicar medidas de control de acceso a los datos de pago únicamente a las personas autorizadas



Convergence
SERVICES