Convergence
SERVICES

ISOs and certifications

The importance of corporate certifications

Convergence
SERVICES

Having international certifications in your company brings diferent benefits, among the main ones is customer satisfaction, as a business strategy.

Being a certi ed company transmits security to customers, as it provides in addition to its main focus “the product / service” and guides the customer goals to perform in the right line based on international standards and on which are measured all companies that are highly competitive, opening the company to greater opportunities.

With this background we will understand the client and guide him to achieve total satisfaction. Through certifications, our client will be able to add value related to quality, relationship, processes, performance, price and benefits.

Having the right certifications reflects that the organization is open to new opportunities and alliances, as well as the care for the customer's information, positioning itself at the same level as the big competitors.

Finally, in the short term, the benefits of a certification and the correct consulting translate into improvements in the internal processes of the organization. It reduces operational errors such as rework, in addition to increasing the quality and conformity of products. Savings impact on the possibility of investing in the development of new and better products, in reforms and upgrades of facilities and equipment or in the acquisition of new technologies.

Convergence
SERVICES

At Convergence Services we are experienced consultants, we accompany our clients before and during the certification process of their company, thus guaranteeing certification and being able to obtain the previously mentioned benefits.

The ISOs and certifications in which we provide consulting and support services are the following:

ISO 27001 Certification

ISO 22301 Certification

SOC Certification

PCI Certification

Convergence SERVICES

ISO 27001 Certification
(ISMS: Information Security Management System)

An Information Security Management System (ISMS) allows organizations to know, manage and minimize risks related to information security in a systematic and efficient way. The proper implementation and certification of this system offers a guarantee of confidentiality, integrity and availability of stored data.
The certification of an Information Security Management System generates customer confidence and improves the efficiency of the company

Benefits:

- Minimize the risks inherent to information security (data loss, theft, corruption, etc.).
- Ensure legal compliance.
- Generate customer confidence by ensuring the good management of the data entrusted to your organization (thanks to its international recognition).
- Protect and ensure the security of their information
- Identify the risks associated with the storage of information.
- Facilitate the understanding of the standard and its integration with other management systems.

the presence of this standard stands out in companies dedicated to information technology services, as well as insurance companies, retailers, companies in the transport sector, governments, etc.

Convergence SERVICES

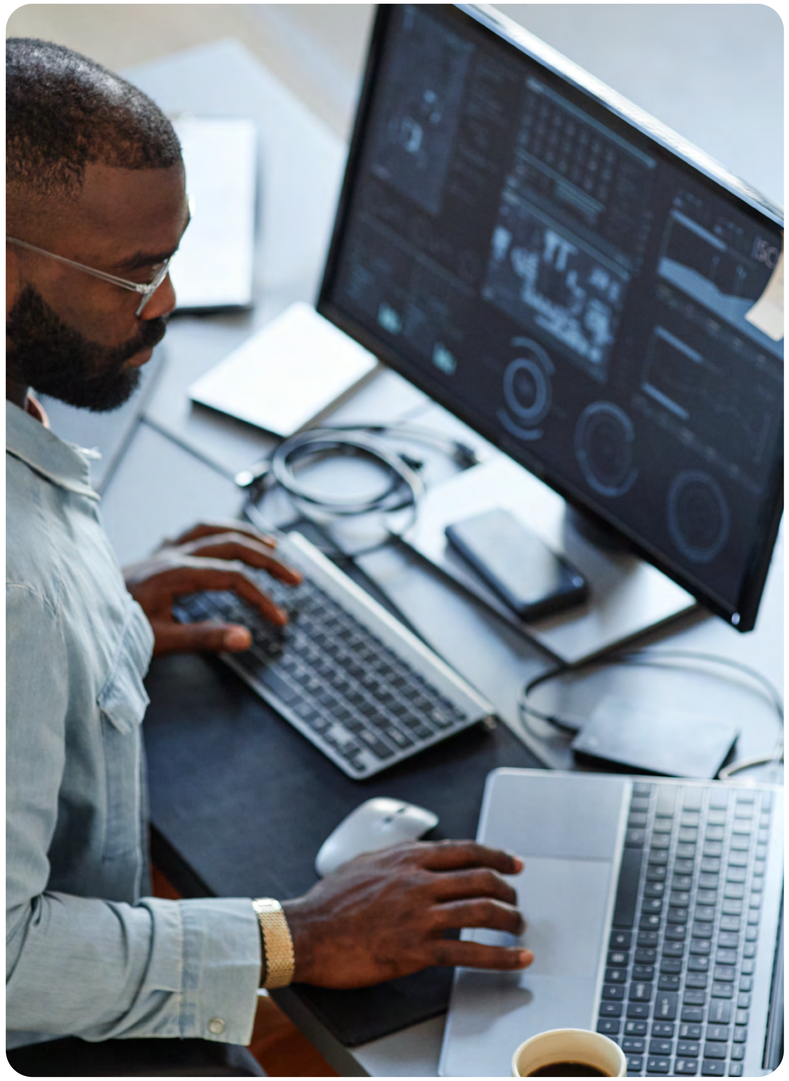
ISO 22301 Certification
(BCMS: Business Continuity Management)

In the event of an emergency, companies must have the ability to mitigate damage and continue operating. ISO 22301 is the international standard for Business Continuity Management (BCMS). Published by the International Organization for Standardization, ISO 22301 is designed to help organizations prevent, prepare for, respond to and recover from unexpected incidents. To achieve this, the standard provides a practical framework for establishing and managing an effective business continuity management system. ISO 22301 aims to protect the organization from a wide range of potential threats and disruptions.

This standard may be suitable for your organization if you need to demonstrate to stakeholders that your organization can quickly overcome any operational disruption in order to provide continuous and effective service.

Benefits:

- Have the ability to resist the effects of an incident (resilience) as well as prevent or avoid possible scenarios arising from a crisis situation.
- Manage the interruption of your activities while minimizing the economic, image or civil liability consequences derived from it.
- Generar confianza en los clientes asegurando la buena gestión de los datos confiados a su organización (gracias a su reconocimiento internacional)
- Reduce the costs associated with the interruption.
- Avoid penalties for breach of contract as a supplier of products or services.
- Have a structured methodology to resume your activities after an interruption.



Convergence SERVICES

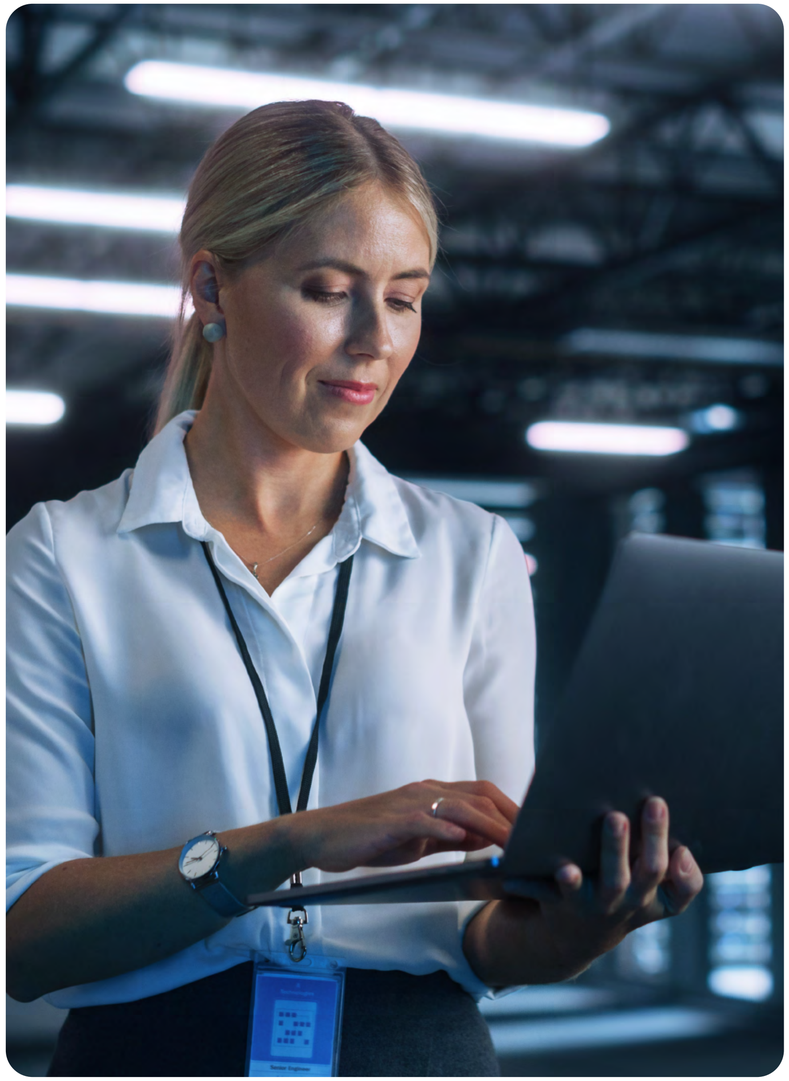
SOC Certification
(Service Organization Controls)

System and Organizational Controls (SOC) for service bureaus are internal control reports created by the American Institute of Certified Public Accountants (AICPA) and included in the AICPA's Trust Service Criteria that facilitate auditing and reporting on the controls a service organization uses to protect information, which helps clients assess and address the risk associated with an outsourced service.

A Service Organization Controls Certification (SOC 2) is an independent audit of a company's security practices. When a company passes a SOC 2 audit, it is showing both potential and existing customers that it has sound cybersecurity practices.

SOC 2 reports capture data security, availability, processing integrity, confidentiality and privacy.

1. **Security:** data protection and system security against unauthorized access and data exposure. Security also includes protection against system damage that could result in loss of data availability, integrity and confidentiality.
2. **Availability:** reliability of the systems required for the entity to be able to continue working normally.
3. **Integrity of processing:** system processing must be complete, valid, accurate, on time and authorized.
4. **Confidentiality:** data classified as “confidential” must be protected so that the entity's objectives can be achieved.
5. **Privacy:** Information must be collected, used, retained, disclosed and disposed of so that the entity's data privacy objectives can be met.



Convergence SERVICES

PCI Certification
(Payment Card Data Security Standard)

In an increasingly digital and interconnected world, protecting sensitive customer information and ensuring transaction security has become essential. One of the main ways for companies to demonstrate their commitment to data security is through security certi cates such as PCI DSS.

Speci cally for companies that process payment card transactions, PCI DSS (Payment Card Industry Data Security Standard) is a security standard established by major payment card companies such as Visa, Mastercard, American Express and others.

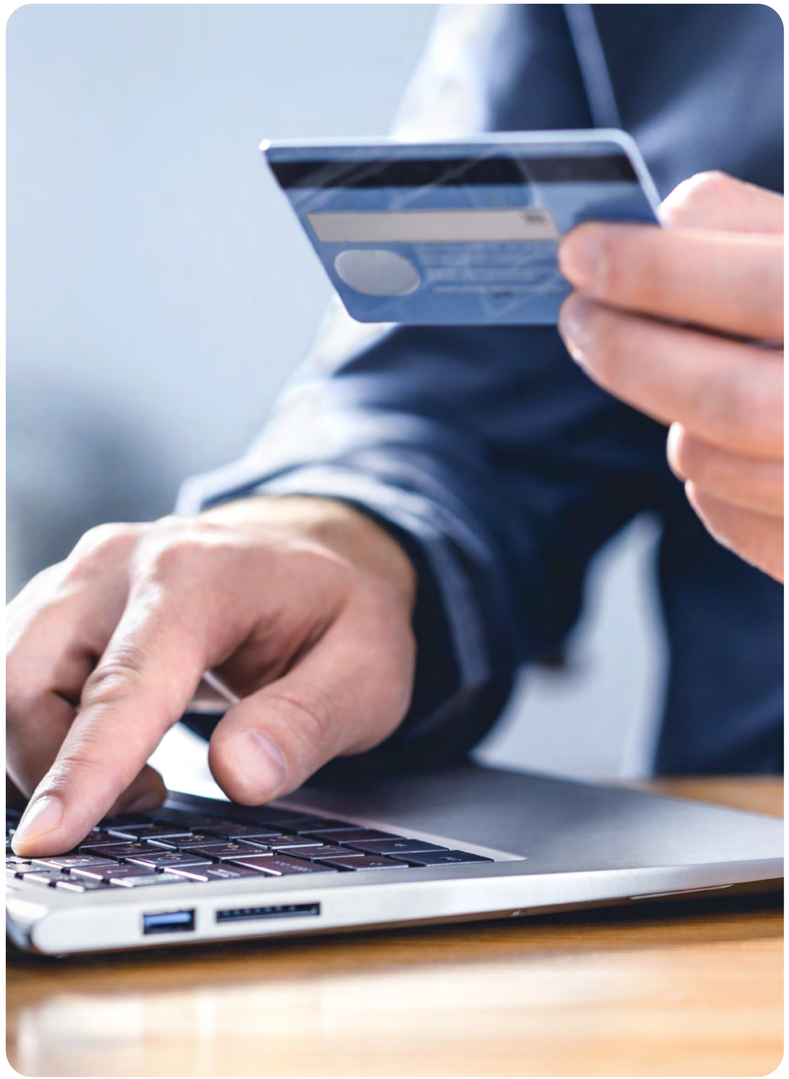
PCI DSS is a set of security requirements aimed at protecting sensitive customer data during end-to-end payment card transactions, meaning that it covers all aspects of the storage, processing and transmission of card data.

By following PCI DSS guidelines, companies can establish a secure environment for transaction processing and, as a result, minimize the potential for security breaches and protect customer confidence.

By obtaining PCI DSS certification, companies demonstrate their commitment to data security and reinforce their security posture by ensuring secure and reliable transactions.

Organizations must meet a number of requirements set by the PCI security council. These are:

- Building and maintaining a secure network infrastructure
- Assessing and analyzing risks to protect cardholder personal data
- Maintain a global security policy covering all aspects of card payment processing.
- Implement measures to control access to payment data to authorized persons only.



Convergence
SERVICES