ISO 27001

senhasegura®

Content

1. Introduction 3

    1.1 Context 3

    1.2 Purpose 4

2. Information Security Management 5

    2.1. Information Security management system 6

3. ISO 27001 Standard 8

4. A PAM Solution and the ISO 27001 Standard 10

5. The senhasegura Solution 14

6. Conclusion 16

1. Introduction

1.1 Context

The growing demand for information makes the correct and effective implementation of Information Security management within organizations today one of the biggest challenges for business continuity in the corporate environment.

To ensure efficient Information Security management - and therefore business continuity - for their interested parties, organizations have been required to implement policies to securely control and manage their information. The policies implemented from the analysis of risks that the company is subject to must address from the definition of Information Security to the roles and responsibilities of those involved in the policy.

In order to certify organizations in Information Security, standards were created to ensure the application and efficiency of Information Security Management controls. These standards propose the use of Information Security Management Systems (ISMSs), which allows the organization to implement processes and controls for the correct Information Security Management.

Thus, the use of standards and regulations such as ISO/IEC 27001 enables companies of all sizes to properly develop and implement information security policies by defining the implementation of an Information Security Management System in the environment, whose goal is to ensure the reliability, availability, and integrity of information. This standard was developed by the International Organization for Standardization (ISO), along with the International Electrotechnical Commission (IEC), and establishes security guidelines and principles to be applied by companies.

Based on the need to ensure the efficient implementation of ISMSs, applications have been developed to help organizations achieve compliance with security laws, regulations, and policies in their Information Security Management Systems. These tools, based on the monitoring of activities within the ISMSs, enable the generation of reports on compliance and the use of corrective actions for nonconformities. Using these tools helps any organization comply with these standards.

Privileged Access Management (PAM) is the aspect of Identity and Access Management that deals with high-privilege users and credentials in an organization. These privileged credentials enable malicious attackers to gain unrestricted access to corporate resources and critical systems, with far greater privileges than a standard user.

As a PAM solution, senhasegura has a series of features to protect an organization, tracking critical actions in the environment, streamlining internal and external audit processes, and making the organization not only in compliance with ISO 27001, but also with a number of regulatory requirements.

1.2 Purpose

This document, therefore, intends to introduce the controls included in ISO 27001, and how systems managed by privileged users will be affected by the standard. In addition, aspects such as Information Security Management and Information Security Management Systems will be presented.

Next, the concepts related to Privileged Access Management and how they are connected with the controls introduced by the 27001 standard will be addressed. Lastly, the way senhasegura, as a Privileged Access Management solution, can help any organization comply with the requirements introduced by ISO 27001 will be covered.

2. Information Security Management

According to the Information Technology Governance Institute (ITGI) principles, corporate information and the technology needed to support it cannot be treated individually, and IT should be considered an integral part of the corporate strategy, rather than simply a means to make it practicable. Thus, for IT, the use of operational risk management is required to ensure complete security and confidentiality of data from 'interested parties' without the institution being compromised. Furthermore, it is necessary to provide a systems infrastructure that ensures the integrity of data and management reports, as well as the adaption of systems and procedures related to the analysis and measurement of operational risk through stored data.

To meet the new challenges of legal and regulatory requirements, institutions are prioritizing investments in Information Security and IT itself.

The scope of these laws includes both methods of failure tolerance for IT infrastructure and protection against hostile actions, as well as ensuring responsible use of resources, seeking greater focus on better and more effective internal controls to ensure risk management in its processes and in relationships with customers, suppliers, and business partners. These controls are defined as policies, procedures, practices, and organizational structures designed to provide reasonable assurance that business goals will be met, and that undesirable events will be prevented or detected and corrected.

2.1. Information Security Management System

The Information Security Management System is part of the organizations' management system. It is based on the business' risk management, with a specific focus on information. The key concept of ISMS is the creation, implementation, and maintenance of a series of management processes for effective Information Security.

The ISMS ensures the confidentiality, integrity, and availability of information aligned with policies, goals, processes, and procedures. For the ISMS to remain effective and efficient over the long term, it needs to be regularly assessed and reviewed. That is the aim of the PDCA (Plan - Do - Check - Act) model proposed by ISO 27001, which ensures continuous improvement processes for the ISMS. The implementation of an ISMS in ISO 27001 is based on a continuous information cycle, the PDCA model, consisting of four stages: Plan; Do; Check; and Act, shown in figure 1 and defined below:

- The Plan stage allows the establishment of the ISMS policy, objectives, processes, and procedures;
- The Do stage deals with the implementation of ISMS policies, objectives, processes, and procedures;
- The Check stage aims to evaluate and measure the ISMS' performance;
- The Act stage allows for the possibility of corrective actions according to the report results.

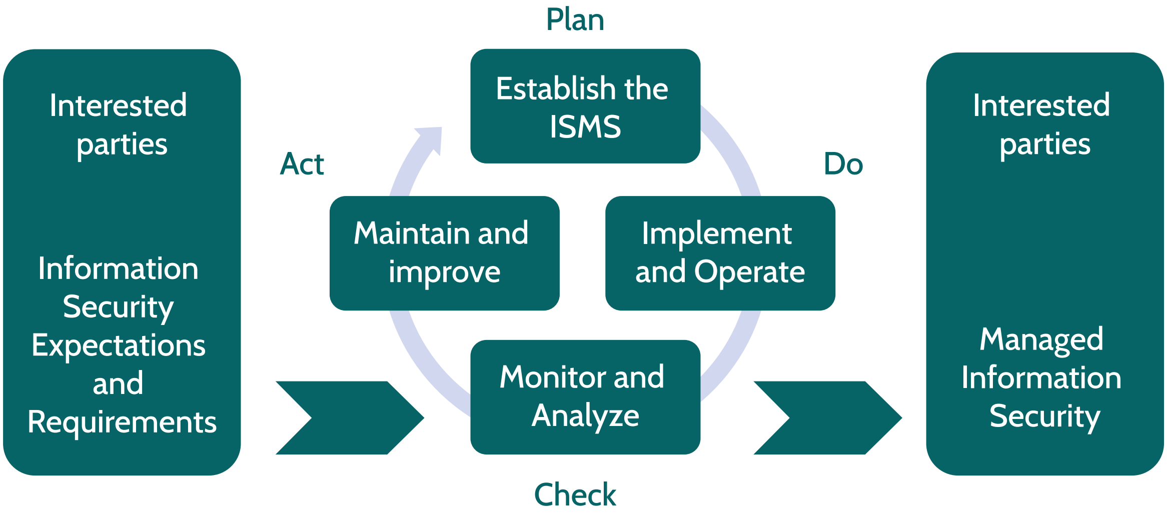

Figure 1 – The PDCA cycle applied to the processes of an Information Security Management System

The use of the PDCA model allows not only to establish, implement and maintain the ISMS, but also to improve the policies, objectives, processes, and procedures that make up the ISMS, thanks to the dynamics of continuous improvement.

This requires an explicit definition of the company's expected results, as well as activities and events required to ensure information security (policies) and a process to measure the performance of organizations in achieving these results (management). One way to ensure this management of information and its security is the use of standards by the organizations to ensure that all steps are taken to achieve effective management. One of the best known and most used standards is ISO/IEC 27001, which will be presented in this document.

3. ISO 27001 Standard

ISO/IEC 27001 is an Information Security Management standard published by ISO in partnership with IEC. The latest version of the standard was published in 2013 and is officially known as "ISO/IEC 27001: 2013, Information Technology - Security Techniques - Information Security Management Systems - Requirements" (ISO 27001). In Brazil, the translation of the standard was published by the Brazilian Association of Technical Standards (ABNT) under the title NBR ISO/IEC 27001:2013.

ISO 27001 identifies a starting point for the development of an organization's specifications and addresses the following topics, in addition to the first four introductory chapters:

4. Context of the Organization – Addresses the understanding of the organization and its context, the needs and expectations of interested parties, and the scope of the Information Security Management System;

5.Leadership – Outlines the roles and responsibilities of top management to ensure the proper implementation of the ISMS;

6. Planning – This topic introduces aspects related to actions to address risks and opportunities, in addition to the objectives of Information Security and plans to achieve them;

7. Support – treats of aspects like resources, competency, awareness, communication and documentation;

8. Operation – This includes aspects such as operational planning and information security risk assessment and treatment;

9. Performance evaluation – Controls related to monitoring, measurement, analysis, and evaluation are proposed, as well as internal audit and review by the top management

10. Improvement – proposes a process of continuous improvement, including the detection of nonconformities and their corrective actions

ISO 27001 is used by organizations worldwide to establish, implement, maintain, evaluate and continually improve an Information Security Management System. This standard specifically identifies the requirements for establishing a framework to achieve the organization's Information Security goals. These specific requirements include leadership commitment and role assignment, and the development of an Information Security policy.

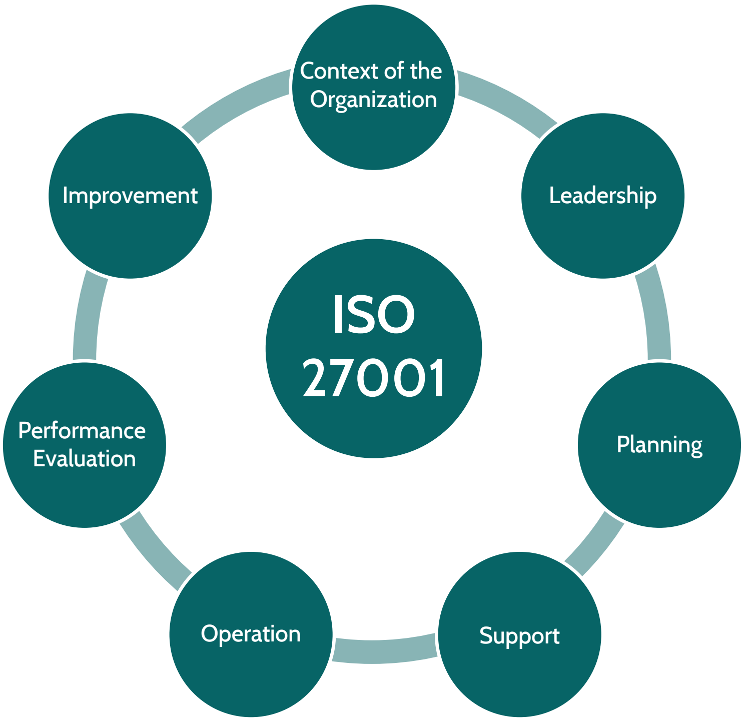

Figure 2 – Aspects addressed in the ISO/IEC 27001 Standard

Lastly, ISO 27001 requires organizations to create their own sets of requirements controls, based partially on a risk assessment to ensure the implementation of all requirements from an ISMS. Also, ISO 27001 provides a comprehensive catalog of control objectives and related controls that an organization can use. At the same time, the standard focuses at the ISO/IEC 27002:2013 standard, which provides a best practice guide that assists in the implementation of an ISMS, making it easier to achieve the requirements specified in the first standard.

4. A PAM Solution and the ISO 27001 Standard

Privileged access is one of the most sensitive aspects of IT. Through administrative credentials, significant changes can be made to critical systems, which in many cases can affect business continuity. The impact of using these privileged credentials in a malicious way can cause serious damage, from violations of compliance items, which can lead to heavy penalties, to security incidents - which result in reduced trust by the interested parties and lost revenue.

In this context, a PAM solution allows the organization to set parameters to control privileged access throughout the environment, and for this reason, it must monitor the implementation of ISO 27001 in any environment. One of the requirements of an ISMS is the full tracking of credentials of own and third-party employees, as well as non-human users, such as credentials embedded in scripts and applications. If these users are able to make unauthorized changes to systems, access sensitive data, and eliminate trails of their privileged actions, the organization is exposed to serious risks.

Then, a PAM solution must be able to:

- Allow a company to set a number of flexible parameters for privileged access control, such as window access, access restrictions for specific users or target systems, or access limitation to resources required to perform a task;

- Be a single repository of administrative credentials across all systems and environments within an organization, resulting in reduced audit time and incident investigations;

- Link role-based user control to critical systems, applications, and services, thus allowing the connection between a privileged user and an individual, which improves the granularity of control and visibility;

- Provide a scalable, searchable and comprehensive audit and reporting solution for user activities on critical systems, with the ability to view commands and sessions on those systems;

- Centralize privilege visibility and control across a single management, policy and reporting platform for all devices and users, resulting in increased efficiency and unification of the management approach across the environment;

- Integrate user activity auditing such as Syslog with other monitoring and reporting technologies such as SIEM;

- Strengthen the policies of least privilege for granular control of administrative rights, while facilitating elevation of privileges without the need to assign administrator or root access;

- Escalate management of all credentials across a range of operating systems and platforms.

From the 35 control objectives included in Annex A of ISO 27001, 28 (or 80%) of them are directly or indirectly linked to Privileged Access Management processes. Some of the controls connected with the functionality of a PAM solution will be listed below:

- **Section A.5 Information Security Policies** – Aims to provide guidance and support for Information Security in accordance with business requirements and relevant laws and regulations.
  This section outlines aspects related to the definition and approval of Information Security policy sets. These policies must be published and communicated to employees and third parties. In addition, the standard proposes a review of the policies implemented to ensure applicability and effectiveness;

- **Section A.6 Organization of Information Security** – The purpose of this section is to establish a management structure for starting and controlling the implementation and operation of Information Security within an organization.
  According to this section of ISO 27001, all responsibilities for Information Security must be properly defined and assigned. Additionally, conflicting duties and responsibility areas should be separated to reduce opportunities for unauthorized or unintended changes or misuse of an organization's assets;

- **Section A.8 Asset Management** – Deals with identifying an organization's assets and defining the appropriate responsibilities for protecting those assets.
  Assets related to information and information processing resources must be identified and an inventory of such assets should be structured and maintained.

- **Section A.9 Access Control** – Aims to limit access to information and information processing resources.
  The controls connected with this section establish that an access control policy must be developed, documented and critically analyzed, based on the information and business security requirements. Besides that, users should only be granted access to networks and network services that they have been specifically authorized to use.

- **Section A.12 Operations Security** – The purpose of this section is to ensure the secure and correct operation of information processing resources.
Detection, prevention and recovery controls should be implemented to protect against malicious software, combined with an appropriate user awareness program. Backups of system information, software, and images must be performed and tested on a regular basis in accordance with the defined backup policy.

- **Section A.15 Supplier Relationships** – Addresses maintaining an agreed level of information security and service delivery in line with agreements with suppliers.
Access by third parties, including from suppliers and partners, should be managed in the same way the access by a company's own employee is managed.

- **Section A.16 Information Security Incident Management** – The purpose of this section is to ensure a consistent and effective approach to managing information security incidents, including reporting on information security weaknesses and events. Information security events should be evaluated, and it must be decided whether they are classified as information security incidents or not. All incidents should be reported through the appropriate management channels, as soon as possible.

Privileged Access Management may be a direct or indirect requirement for compliance programs and standards, including ISO 27001, which typically require organizations to demonstrate proper system access management. Lastly, all actions taken through privileged sessions can be recorded and used for audit purposes.

5. The senhasegura Solution

senhasegura is a software and hardware solution that stores, manages, and monitors all credentials, such as passwords, SSH keys, and digital certificates in a secure, tamper-resistant location. By using encryption mechanisms, senhasegura offers users the ability to access a series of credentials registered in the solution. In addition, through senhasegura, one can safely access all network resources through a series of protocols, storing all usage records for audit and compliance analysis purposes. Its intelligence allows the real-time analysis of the actions taken by users and the generation of alerts to identify frauds or inappropriate actions.

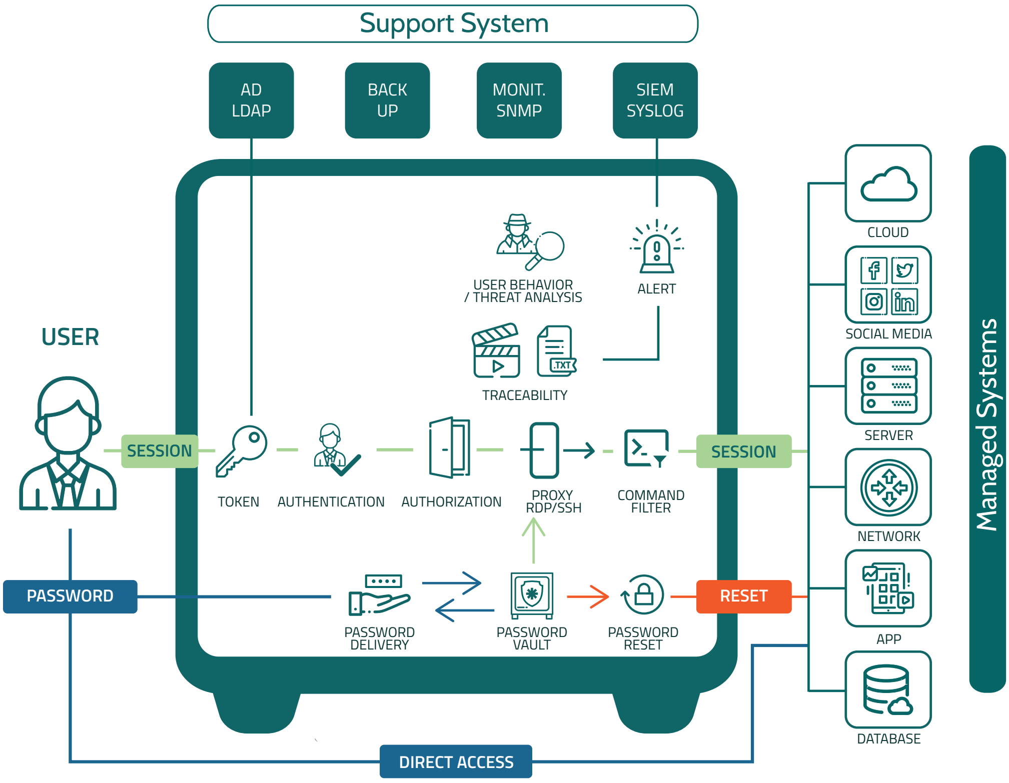

Figure 3 – Privileged Access Management Flow through senhasegura

senhasegura allows companies to implement all controls included in ISO 27001 that are related to privileged account security. Its centralized management and reporting capabilities enable IT professionals, auditors, and certifiers to easily verify privileged account management and control, thus reducing the cost of these assessments.

To make it easier to understand, the controls previously presented will be linked with the solution's respective features:

Seção	Controle	Funcionalidade
A.5 Information Security Policies	A.5.1 Management direction for information security	senhsegura ensures proper definition and enforcement of security policies related to privileged access
A.6 Organization of Information Security	A.6.1 Internal organization	In the senhasegura solution, one can define and assign roles and responsibilities, as well as the separation of duties, through the use of Access Groups, ensuring the concept of least privilege
A.8 Asset Management	A.8.1 Responsibility for assets	senhasegura's Scan Discovery feature scans and analyzes the entire network to discover devices and their credentials
A.9 Access control	A.9.2 User access management	senhasegura allows the allocation and use of administrative privileges in a restricted and controlled manner. Through the solution, one can to assign, review and revoke accesses
	A.9.4 System and application access control	Through senhasegura, one can eliminate direct access to critical systems. Thus, all access to these systems must pass through the solution
A.12 Operations security	A.12.2 Protection from malware	With the use of the passwords.Go! complement installed on workstations, one can run applications that require privileges with vault-managed credentials without the user knowing their password, thus protecting the environment from malicious software
	A.12.3 Backup	Through senhasegura, one can eliminate direct access to critical systems. Thus, all access to these systems must pass through the solution

Seção	Controle	Funcionalidade
A.12 Operations Security	A.12.4 Logging and monitoring	All the privileged accesses made through senhasegura, besides all the actions executed in the environment are stored in logs, in inviolable environment, which allows the administrators to have a complete visibility of all the actions executed in systems and devices
A.15 Supplier Relationships	A.15.1 Information security in supplier relationships	Through senhasegura, it's possible to stablish segregate policies for third-party access to the environment. The session management resource creates detailed audit tracks, including about remote accesses.
A.16 Information Security Incident Management	A.16.1 Management of information security incidents and improvements	senhasegura gives administrators accurate information about privileged sessions thanks to its traceability and monitoring capabilities. Thus, they get full details of how and why a security incident has occurred, enabling quick and effective corrective actions

6. Conclusion

In the information society, while information is considered to be one of an organization's main assets, it is also at constant risk.

Security measures implemented by organizations to ensure Information Security include security policies, which aim to define standards, procedures, tools, and responsibilities that must be followed by users of organizations. Security policy is the basis for all information protection issues, playing an important role in organizations.

The use of standards and regulations such as ISO 27001 enables companies of all sizes to properly develop and implement information security policies. ISO 27001 provides a code of good practice for implementing an Information Security Management System in the organizational environment, which aims to ensure the reliability, availability, and integrity of information.

In this context, a PAM solution assists any organization wishing to comply with the controls included in ISO 27001. Therefore, besides the security benefits brought by a PAM solution, this type of tool performs the direct and indirect execution of those controls. In this way, organizations that connect the implementation of a PAM solution with the ISO 27001 compliance process can experience a fast and manageable process.

When used to manage privileged access on organizational systems and platforms that store or protect the integrity of sensitive data, senhasegura enables organizations to automate a range of controls and control groups related to unauthorized access to systems within the scope of ISMS. Through an agentless architecture, the solution provides a centralized access point for critical systems. Its features allow strengthening the access control, limiting the user access only to what was previously authorized, respecting the principle of least privilege. Thus, senhasegura offers full visibility of who has access to these systems and what actions have been taken through privileged credentials. Finally, control and visibility over privileged actions are key factors for the organization to be ISO 27001-compliant.

Click here!

I WANT TO SCHEDULE A DEMO!