



INSTITUTIONAL DECLARATION

PSRH, hereinafter "the Organization" or "the business," whose mission is to provide excellence in the optimal and efficient resolution of complex and high-impact problems for the clients it represents, both nationally and internationally.

As a result, it follows that the core activity of the Organization is the collection and processing of highly sensitive client information, as well as information from complementary external sources, with the aim of providing comprehensive advice in these matters, meeting the expectations and requirements of its clients, both in terms of service level and professionalism during the process.

In this way, PSRH declares that its most valuable assets are its corporate image and reputation, which primarily rest on the fundamental principle of confidentiality of the information handled with each of its clients, thereby forming a healthy and trust-based relationship with each of them.

As a consequence, the Organization recognizes that information is also a highly relevant asset, categorizing it as a critical and valuable element for fulfilling its mission. Proper management of this information is an essential catalyst for preserving its prestige, trust, and professionalism, which contribute to the Organization's image.

For this reason, PSRH will establish an integral and transversal process throughout the organization for the construction of information security and cybersecurity. This process will operate through the implementation of an Information Security and Cybersecurity Management System, hereinafter referred to as the ISCMS, which will ensure compliance and operation of mechanisms focusing on the identification, protection, detection, response, and recovery from possible incidents that could negatively affect key areas such as transparency, reputation, image, and the operation of PSRH.

In this context, through its ISCMS, PSRH will continuously strengthen and improve its control environment, ensuring the implementation of effective measures and improvements that, in a consistent manner, will raise the Organization's maturity level in information security and cybersecurity. In this way, the goal is to maintain the value of the information over time, preserving aspects such as confidentiality, integrity, availability, authenticity, and privacy of institutional information assets that are relevant or critical to the operation and prestige of the Organization.

Institutional Declaration (Continued)

Finally, based on all that has been outlined above, it is part of PSRH's institutional declaration to consider the process of building information security and cybersecurity directly as a strategic catalyst for achieving the business objectives.

Objectives

The objective of this policy is to formalize PSRH's institutional declaration regarding information security and cybersecurity, thereby outlining the general guidelines that the Organization must follow for the implementation, maintenance, and improvement of the information security and cybersecurity building process at the organizational level, considering processes, technology, and the people involved.

Scope

This document represents the institutional declaration that establishes the Information Security and Cybersecurity Management System (ISCMS), as well as the general guidelines supporting the process of building information security and cybersecurity at PSRH. As a result, this document applies to all other documents derived from this policy, as well as any control measures aimed at preserving the confidentiality, availability, integrity, authenticity, and privacy of information assets.

In addition to the above, this policy must be applied by all individuals who are part of PSRH, whether they are in operational or administrative areas, employees or third parties, who, due to the fulfillment of their responsibilities, have partial or full access to the Organization's information.

Thus, in accordance with the provisions of NCh ISO 27001:2012, this document applies to the following controls:

- **A.5.1.1 – Information Security Policy**

Roles and Responsibilities

Information Security Officer: This role will be responsible for ensuring the application and compliance with the provisions outlined in this policy, as well as for conducting the necessary reviews and modifications to maintain its coherence and suitability in relation to the business and its constant changes.

Information Security Committee: This will be the body where all changes and modifications to this policy will be approved and formalized.

Users: These roles will be responsible for internalizing and executing the guidelines set forth in this policy, as well as reporting any non-compliance or potential risks that may violate what is stated in this document.

SPECIFIC OBJECTIVES OF THE INFORMATION SECURITY AND CYBERSECURITY MANAGEMENT SYSTEM (ISCMS)

Regarding**Confidentiality**

PSRH must verify the implementation of necessary controls to safeguard information assets from unauthorized access, accidental disclosures, espionage, and other similar actions, whether accidental or deliberate.

Regarding**Integrity**

PSRH must verify the implementation of necessary controls to protect information assets from any degradation caused by internal or external agents, environmental factors, or manipulation that could affect their accuracy and completeness.

Regarding**Availability**

PSRH must verify the implementation of necessary controls to protect information assets from any partial or total disruption, ensuring that they remain accessible and usable by authorized users, so as not to affect operational continuity.

Regarding**Authenticity**

PSRH must verify the implementation of necessary controls to safeguard information assets, ensuring they do not lose their validity and usability. This includes ensuring non-repudiation, i.e., the ability to prove that a user or application is truly who they claim to be.

Regarding Privacy

PSRH must ensure the implementation of necessary controls to protect information assets and maintain their privacy characteristics, in compliance with constitutional guarantees, establishing requirements for the handling and use of information in accordance with current legislation. Therefore, the Organization must not only address regulatory requirements regarding personal information but also develop mechanisms and strategies to ensure its proper management, including aspects such as its collection, use, processing, storage, and disclosure.

GENERAL FRAMEWORK OF THE ISCMS: RISK MANAGEMENT

Given the characteristics of the institution described above, PSRH understands that its core activity is the handling of sensitive information that is highly relevant to the interests of its clients. Any incident involving this information directly harms the trust these clients place in the Organization, and, consequently, affects its image and reputation. Therefore, it is declared that the management of information assets that flow through its processes must be structured and secure throughout their entire lifecycle, with the following general stages being highlighted:

- **Information Collection:** This encompasses the reception of both preliminary information from the client or representative regarding a matter, as well as the information necessary to delve deeper into the issue and provide counsel, whether provided by the client or collected from external sources.
- **Information Storage:** This refers to the storage and protection of information over time, including both the information provided by each client and the historical information generated during the advisory services provided by the Organization.

- **Information Creation:** This includes all information, documents, or information assets generated from the execution of a service or advisory to a client or representative of the Organization.
- **Information Presentation:** This covers any act of publication, delivery, or display of information related to a matter to any natural or legal person who is not part of the professional relationship between the client and the Organization.

Es así, como **PSRH** reconoce que cualquier vulneración a la seguridad de los activos de información, en cualquiera de las etapas descritas anteriormente, podría suponer como consecuencia, un cuestionamiento hacia la Organización, tanto a nivel de imagen / reputacional, desde el punto de vista de la confianza del cliente hacia la organización, así como a nivel operacional, desde el punto de vista del servicio de excelencia que debe mantenerse hacia sus representados dada la alta criticidad de los asuntos que manejan. Dado lo anterior, y, con el fin de velar por el cumplimiento de lo establecido en la declaración institucional de este documento, **PSRH** justifica el establecimiento de un SGSIC.

Para dar cumplimiento a lo estipulado en esta política, **PSRH** a través de su Sistema de Gestión de Seguridad de Información y Ciberseguridad (SGSIC), deberá implementar y mejorar de forma continua en el tiempo, procesos, procedimientos, y mecanismos que conformen su ambiente de control de seguridad de información y ciberseguridad, y cuyo objetivo principal sea disminuir los niveles de exposición riesgos de este tipo que presente el negocio. Esta implementación, debe realizarse, en primer lugar, de forma consistente con los niveles de riesgo que presente la organización, y, en segundo lugar, debe realizarse de forma coherente con el nivel de madurez en estas temáticas que presente la Organización y su evolución en el tiempo, velando por enfocar los esfuerzos en una primera implementación de controles de tipo higiénicos y basales, para de esta forma generar capacidades de tipo fundamentales que representan los cimientos para de forma posterior, lograr la optimización de los esfuerzos y recursos de **PSRH** al momento de implementar mecanismos de control que requieren de estas capacidades fundamentales para su implementación eficiente, y apunten directamente a la resiliencia organizacional. De forma general, y, desde un enfoque de alto nivel, los procesos de control que la Organización debe considerar como parte de su ambiente de control son los siguientes:

Baseline Control Processes

These correspond to control processes that, although not necessarily related to information security, are of utmost importance in the process of building security, as they represent the foundations upon which more mature organizational control processes can be constructed. These processes focus on identifying the critical components for the organization, among which the following should be considered at a minimum:

- **Identification of key processes for the operational maintenance of PSRH**, with the aim of establishing the organization's value chain, thereby determining the initial scope of the ISCMS.

- **Classification of business processes** based on the impact that the unavailability of each of these processes would have on the business (Business Impact Analysis – BIA).

Identification of Information Assets

- **Identification of all information assets** received, stored, processed, and issued by PSRH. These assets may exist in various media and formats, both physical and digital.
- **Classification of the identified information assets**, based on the parameters of confidentiality, integrity, availability, authenticity, and privacy, in order to categorize them according to their degree of criticality to the institution. This operation should involve all operational lines that constitute the organization's value chain.
- **Identification of the technology associated with the information assets**. This process must be as continuous and real-time as possible, managed through the implementation of an updated inventory of technological components that support the organization's operations.
- **Establishment of a mapping** that links the business processes constituting the value chain, the information assets that flow through them during the organizational operation, and the technology that supports them, which in turn underpins the execution of these relevant business processes.
- **Conducting risk analyses on information assets** with medium and high levels of criticality. These analyses should at least consider the following indicators: the value or criticality of the information asset, the weight of vulnerabilities associated with the technology, and the weight related to threat typology or the capture of threat indicators for the technology associated with PSRH's critical processes. This process will provide a more detailed view of where the Organization should focus its efforts to reduce or maintain the risk to the business's reputational and operational image.
- **Implementation of the ISCMS** aligned with market best practices in these areas, in accordance with compliance derived from associations, partnerships, strategic memberships, regulations, laws, and government decrees that may apply to the scope in which the Organization operates. The Information Security and Cybersecurity Management System must incorporate governance definitions, including roles and responsibilities related to the implementation, maintenance, and continuous improvement of the control environment in these areas.
- **Determination of the specific scope and objectives of the ISCMS**, based on the risk analysis. This scope must be defined according to high-impact risks, or those that could negatively affect the achievement of the institution's objectives, its operations, reputation, image, and/or client trust.

Hygienic Control Processes

These correspond to control processes that represent a higher level of organizational maturity in these areas and focus directly on protective measures for the organization's critical components, as well as the detection of potential incidents or failures in the aforementioned protections. Some of the key topics to consider at a minimum for these types of processes are:

- **Information security and cybersecurity of human resources.**

- **Management of information assets according to their criticality classification.**
- **Risk management of information assets.**
- **Establishment of protection mechanisms and measures for critical information assets.**
- **Establishment of mechanisms and best practices for information security** related to the development and/or acquisition of software and technology.
- **Establishment of mechanisms and monitoring measures** for information assets and identification of potential incidents.

Control Processes for Resilience

- **Vulnerability management and remediation of gaps.**
- **Establishment of mechanisms and response measures** for incident containment.
- **Establishment of advanced threat management mechanisms.**
- **Establishment of mechanisms and measures for recovery and returning processes and systems to normal operations** in the event of potential incidents.

Awareness and Culture in Information Security

PSRH recognizes that an essential part of executing the process of building security is the people who make up and are part of the organization. Therefore, it is declared that topics related to awareness, training, education, and culture in these areas are of utmost importance for the business objectives related to information security and cybersecurity.

Thus, the Organization must establish processes, mechanisms, and measures to promote awareness and training in these areas, with the goal of progressively changing the institutional culture and raising the levels of awareness in information security and cybersecurity.

Functional Structure of Information Security and Cybersecurity

To comply with the provisions in this policy, PSRH must implement governance to manage information security and cybersecurity within the institution and ensure the growth in maturity of corporate security. This governance should be based on the determination and assignment of clearly defined roles for these purposes. Therefore, the Organization will incorporate the functions and responsibilities that each role assumes within the organization into the job profiles, to ensure proper management of information security within the institution.

Functional Structure of the ISCMS

In addition to the above, PSRH will have a functional structure for the ISCMS, which will include at least the following:

- **Information Security Committee** or an equivalent committee, with the goal of monitoring and managing these topics.

- **Role specifically responsible** for information security and cybersecurity issues.
- **Administrative roles** for information security and cybersecurity.
- **Executive roles** for information security and cybersecurity.
- **Team roles.**
- **User roles.**

The responsibilities and functions of this structure will be formally described in a document outlining the creation and appointment of the functional structure for the ISCMS.

Analysis and Evaluation

The General Information Security and Cybersecurity Policy must be evaluated by the Information Security Committee, or the designated body within the organization responsible for monitoring and managing these topics, at least once a year and/or when a significant change or incident occurs that impacts the policy. The purpose of this evaluation is to review and assess its content and direction, ensuring the continuous adequacy, efficiency, and effectiveness of the Information Security and Cybersecurity Management System.

Changes to the General Information Security Policy will be approved by PSRH's Information Security Committee.

Policy Communication

The General Information Security and Cybersecurity Policy of PSRH must be communicated through the official communication channels of the Organization to its staff and anyone who has access to its information assets.

Additionally, access to the policy must be ensured for all collaborators within the organization through its document management system.

Sanctions and Disciplinary Process

Failure to comply with the provisions of this policy will be considered a serious breach of the employment contract obligations and will entitle the employer to terminate the employment relationship without any compensation. The employee will not be able to use as a defense the fact that they have not been previously sanctioned for a similar incident.