SGFGlobal

CORPORATIVE POLICY
SECURITY OF THE INFORMATION

I. Introduction

Information is a strategic asset for SGF GLOBAL, as a company whose recruitment activity in offices around the world depends on IT (Information Technology) systems to achieve its strategic objectives.

These systems must be administered diligently, taking adequate measures to protect them against accidental or deliberate damages that may affect the availability, integrity, confidentiality, authenticity, or traceability of the information processed or the services provided.

The objective of information security is to guarantee the quality of the information and the continuous provision of services, acting preventively, supervising daily activity and reacting promptly to incidents.

IT systems must be protected against rapidly evolving threats with the potential to affect the availability, integrity, confidentiality, authenticity, traceability, intended use, and value of information and services. To defend against these threats, a strategy that adapts to changes in environmental conditions is required to ensure the continuous provision of services.

This implies that the security measures required by different Information Security Management Systems of the countries where we have a presence must be applied.

SGF GLOBAL, carries out continuous monitoring of the criteria and requirements established in the applicable legislation.

Following the best practices, the existence of three differentiated figures that are part is established, being:

- Responsible for the information: It will determine the requirements of the information processed.
- Responsible of protecting the information: Determine what information should be safeguarded for future occasions.
- Responsible for the service: It will determine the requirements of the services provided.
- Security manager: Will determine the decisions to satisfy the information and service security requirements.

SGF GLOBAL must ensure that information security is an integral part of every stage of the IT systems life cycle, from conception to decommissioning, through development or acquisition decisions, and operational activities. Security requirements and financing needs should be identified and included in the planning, in the request for offers.

II. Object

SGF GLOBAL defines this Information Security Policy which fundamental objective is to guarantee the security of the information and the continuous provision of the services it provides, acting preventively, supervising the activity, and reacting diligently in the face of incidents that may occur.

This Policy should lay the foundations so that the access, use, custody and safeguarding of the information assets, which SGF GLOBAL uses to carry out its functions, are carried out, under security guarantees, in its different dimensions:

- Availability: property or characteristic of the assets consisting in the authorized entities or processes having access to them when required.

- Integrity: property or characteristic that the information asset is not altered in an unauthorized manner.
- Confidentiality: property or characteristic consisting of in that the information is neither made available, nor revealed to unauthorized individuals, entities, or processes.
- Authenticity: property or characteristic consisting of an entity being who it claims to be or guaranteeing the source from which the data comes.
- Traceability: property or characteristic consisting of in that the actions of an entity can be attributed exclusively to that entity.

Under these premises the specific objectives of Information Security in SGF GLOBAL will be:

- To ensure the security of the information, in the different dimensions described above.
- Formally manage security, based on risk analysis processes.
- Prepare, maintain, and test the availability and continuity plans of the activity that are defined for the different services offered by the organization.
- Carry out adequate management of incidents that affect information security.
- Keep all staff informed about security requirements and disseminate good practices for the safe handling of information.
- Provide the security levels agreed with third parties when information assets are shared or transferred, depending on the area to which the information belongs and its relevance.
- Comply with the regulations and regulations in force in each country where we operate.

The Security Policy:

- It will be formally approved by the Board of Directors of each country where we operate, according to local regulations in the area.
- It will be reviewed regularly, in a way that adapts to new technical or organizational circumstances and avoids obsolescence.
- All employees and external companies will be informed that they work with SGF GLOBAL, and the corresponding certificates will be delivered.

III. Mission

The purpose of this Information Security Policy is to protect the information and services of SGF GLOBAL.

1. SGF GLOBAL expressly recognizes the importance of information, as well as the need for its protection, as it constitutes a strategic and vital asset, to the point of endangering the continuity of the organization, or at least causing very serious damage. important, if there is a total and irreversible loss of certain data.
2. Information and services are protected against loss of availability, integrity, confidentiality, authenticity, and traceability.
3. The service requirements regarding information security and information systems are met, according to the area to which the company belongs.
4. The controls will be proportional to the criticality of the assets to be protected and their classification.

5. The responsibility for the security of the information involved in the provision of the services included in the scope lies with the Management, which will put the appropriate means, without prejudice to the employees or users assuming their part of responsibility with respect to the means that uses, as indicated in the policies, regulations, and supplementary procedures.
6. Those who perform the Information Security function and other related administration functions, will be those who administer the security.
7. Those responsible for the information have been identified, who should promote the establishment of controls and measures aimed at protecting the data that comprise it, especially those of a personal or critical nature.
8. An information classification system has been established within the regulations, with different levels.
9. The necessary and adequate means have been established and made available for the protection of people, data, programs, equipment, facilities, documentation, and other supports that contain information, and, in general, of any SGF GLOBAL asset.
10. Those who do not comply with what is determined in these regulations and in the complementary procedures may be sanctioned in accordance with the labor legislation and the reference collective agreement in their country, or with personalized sanctions if they are linked to SGF GLOBAL under non-labor contracts, in accordance with the clauses that appear in said contracts and the applicable legislation in the latter case.
11. Risk assessments are carried out periodically and, based on weaknesses, it is determined whether it is necessary to draw up plans to implement or strengthen controls.
12. The dissemination of information and safety training to employees and collaborators is encouraged, preventing the commission of errors, omissions, fraud, or crimes, trying to detect their possible existence as soon as possible.
13. SGF GLOBAL staff must know the norms, rules, standards, and procedures related to their job, as well as their functions and obligations.
14. Security incidents are reported and dealt with appropriately.

IV. Scope

This Security Policy applies to all the offices that make up SGF GLOBAL and its information systems and assets:

- To all departments, both their managers and employees.
- To contractors, clients or any other third party that has access to the organization's information or systems.
- To databases, electronic and paper-based files, treatments, equipment, supports, programs, and systems.
- To the information generated, processed, and stored, regardless of its support and format, used in operational or administrative tasks.
- Information transferred within an established legal framework, which will be considered as proprietary for the exclusive purposes of its protection.
- To all the systems used to administer and manage the information, whether owned or rented or licensed by it.

V. Regulations

The regulations and legislation for the application of this security policy that is included within the Information Security Management System of SGF GLOBAL, is governed and referenced, among others, by the following regulations and laws:

- Law 1581 of 2012 constitutes the general framework for the protection of personal data in Colombia.
- Law 1341 of 2004: Information and Communication Technologies, its general regulations, the competition regime, and the protection of the User
- Business Confidentiality: Decision 486 of the Andean Community, in article 260.
- Labor Code.
- Civil Code.
- Federal Law on Protection of Personal Data Held by Private Parties (“Data Protection Law”).
- General Law on Protection of Personal Data Held by Obliged Subjects.
- Federal Labor Law
- Federal Civil Code

This regulatory framework may entail updates, due to legislative changes. Therefore, in internal regulations an annex to the policy will be created to establish all the updates to the Regulatory Framework. Such updates will be made.

VI. Content

SGF GLOBAL establishes a regulatory body around Information Security to allow the deployment of all those regulatory resources that allow the capacities and legal protection to respond to the mission established by the Directorate.

To obtain this efficiency, a system is established to be managed at three main functional levels: strategic, tactical and operational.

In addition, a technical level is added to adapt the standard to the technological evolutions of Information Systems.

The following are the three levels present in a planning system, plus the technical level adapted to the Information Systems resources:

6.1 Regulatory governance

6.1.1 Strategic level or Higher level

It corresponds to the planning that is oriented to achieve the objectives of the organization and its purpose is to establish the action plans for the operation of the company. It is based on deciding the objectives of the company, defining the resources that will be used and the policies to obtain and manage those resources.

This level establishes the general, but not detailed, framework for the operation of SGF GLOBAL.

The strategic level is conducted by the systems department with its expert Cybersecurity staff, who represent and approve it.

Validation, as final documentary approval, falls to the General Directorate.

6.1.2 Tactical level or medium level

It develops in detail the planning of the operation of each of the areas of SGF GLOBAL based on the reference framework developed at the strategic level.

This level is drawn up by the director responsible for an area, approved by the systems department and validated by Cybersecurity experts.

The basic difference with the strategic level is that the first refers to a policy that affects the entire company and extends over time, while the second refers to a specific standard in the use of a product, service, general operations, quality metrics or others offered by the organization with specific times and deadlines.

6.1.3 Operational level or Lower level

It corresponds to internal rules that allow the execution of tasks in a coordinated manner with other SGF GLOBAL departments that make up the company. It is developed from the guidelines provided by the strategic and tactical planning levels. This level is created and approved by managers responsible for the areas and, for their knowledge, it is submitted to the systems department and its Cybersecurity experts.

Those in charge of writing this documentation must follow the higher standards and abide by rules precisely defined by the other two levels.

The internal standard at this level covers specific time periods according to each process.

6.1.4 Functional level or technical level

Corresponds to technical documentation that allows a worker to use a SGF GLOBAL Information Systems tool that is being implemented to provide service to the worker.

The creation depends on a person in charge and its publication should only appear in the INTRANET of SGF GLOBAL.

6.2 Normative structure

For this, the following regulatory body is established, from highest to lowest rank:

- Higher or Strategic Level:
    - Corporate Policy
- Medium or Tactical Level
    - Corporate Regulations
- Lower or Operational Level:
    - Corporate Procedures
- Technical level:
    - Technical Guides
    - Internal manuals

- Manufacturer’s manuals

6.3 Policies

SGF GLOBAL must be prepared to prevent, detect, react, and recover from incidents, in accordance with the policies established in the service level agreements committed to its clients and users.

In addition, in this document, we will deal with how SGF GLOBAL addresses Information Security policies, how it organizes security in the corporation, how it guarantees and protects personal data, risk management and the development of the security policy. information security.

6.4 Prevention

SGF GLOBAL undertakes to use all the means at its disposal to avoid, or at least prevent as far as possible, that the information or services are harmed by security incidents. For this, the necessary security measures will be implemented determined by the applicable legislation, the controls deemed necessary and established.

To guarantee compliance with this policy, SGF GLOBAL will provide the necessary organizational and technical means to:

- Authorize the systems before going into operation.
- Regularly assess security, including evaluations of configuration changes made on a routine basis.
- Guarantee that the risks that SGF GLOBAL may be affected by are identified and are below acceptable levels.
- Ensure that the services that SGF GLOBAL provides to its clients and the activities that it develops for their provision, have an increasing level of security, and have passed through the necessary tests to guarantee an acceptable level of risk.
- Develop and implement all the necessary policies, controls, and standards in the field of information security to guarantee compliance with business requirements, committed service level agreements and the expectations of interested persons.

6.5 Detection

Since services can quickly degrade due to incidents, ranging from a simple slowdown to a stop, it is necessary to continuously monitor the operation, to detect anomalies in the levels of service delivery and act accordingly.

Monitoring is especially relevant when establishing lines of defense.

Detection, analysis and reporting mechanisms will be established that reach those responsible, both regularly and when there is a significant deviation from the parameters that have been preset as normal.

6.6 Response

SGF GLOBAL:

- Establishes mechanisms to respond effectively to security incidents managed by Cybersecurity experts from SGF GLOBAL's systems department.
- It makes available to its customers and users a point of contact for the communication of incidents detected in its operations, systems@sgfglobal.com
- Establishes in the relationship models protocols for the exchange of information related to incidents with customers and suppliers.

6.7 Recuperation

To guarantee the availability of critical services, SGF GLOBAL has developed continuity plans for ICT systems as part of its general plan for service continuity and recovery activities.

VI. Security organization

SGF GLOBAL establishes committees whose roles will be detailed later for information security management and supervision.

- Corporate Cybersecurity Committee – CCC
- Data Protection Committee – CPD
- Data Protection Officer - DPO

7.1 SGF GLOBAL Corporate Cybersecurity Committee

SGF GLOBAL's Corporate Cybersecurity Committee (CCC) has been established at the direct initiative of its Management and is constituted as a collegiate body to lead and coordinate information security at SGF GLOBAL, ensure governance and risk management cybersecurity, and take actions to safeguard and mitigate these.

Security in the design, implementation, review and improvement of cybersecurity policies and processes.

7.1.1 Mission

The mission of the SGF GLOBAL Corporate Cybersecurity Committee (CCC) is to support the objectives and goals of each one of the offices that make up SGF GLOBAL, providing leadership to guarantee the legality, confidentiality, integrity, availability and traceability of its resources. information, as well as ensuring the non-commitment of third-party assets (Clients) accessible by SGF GLOBAL's own activity with its information systems (in person or remotely).

We understand by information: The information itself, as data managed in the systems that support it, transmitted through digital processes (networks, applications or any type of mechanism used for interoperability with the target systems) or that are stored in storage devices.

7.1.2 Objectives and functions

The Corporate Cybersecurity Committee will have the following objectives and functions:

- Promote continuous improvement of the Information Security Management System.
- Prepare the SGF GLOBAL evolution strategy about information security.

- Coordinate the efforts of the different departments in the area of information security, to ensure that the efforts are consistent, aligned with the strategy decided on the matter, and avoid duplication.
- Prepare (and regularly review) the Information Security Policy for approval by the Management.
- Approve the information security regulations, whether owned by SGF GLOBAL or third parties.

The processes, applications and information systems that support them and that are the object of SGF GLOBAL's own activity.

In short, the awareness of all SGF GLOBAL staff about cybersecurity risks, the protection of SGF GLOBAL information resources, the investigation of possible misuse of the systems, the supervision of compliance with all policies established, procedures and regulations regarding the acceptable and appropriate use of resources, as well as the governance of the security mechanisms that are derived for the protection and defense of the target systems against technological threats that could materialize and compromise the own business or third parties.

The Corporate Cybersecurity Committee belongs to the management bodies and transversal services that SGF GLOBAL provides to all divisions belonging to the group, reporting directly to the Directorate that is responsible for the formalization of cybersecurity policies and objectives. SGF GLOBAL, aligned with the strategic objectives of the company.

- Approve the training and qualification requirements of those responsible for areas, technicians, and users from the point of view of information security.
- Monitor the main residual risks assumed by SGF GLOBAL and recommend possible actions with respect to them.
- Ensure the coordination of the different departments in the management of information security incidents.
- Promote audits to verify compliance with security obligations.
- Approve SGF GLOBAL information security improvement plans. It will ensure the coordination of different plans that can be carried out in different departments.
- Prioritize security actions when resources are limited.
- Resolve the conflicts of responsibility that may appear between the different managers, raising those cases in which it does not have sufficient authority to decide.
- Regularly report the status of information security to the Management, through monthly reports (Corporate CIBERSECURITY Reports) and meeting minutes.

7.2 Data Protection Committee

SGF GLOBAL, to guarantee the correct management of personal data processing, has set up the "Personal Data Protection Committee" under the Directorate, which will assume the responsibilities of the Personal Data Protection Management System.

7.2.1 Objectives and functions

The Personal Data Protection Committee will have the following objectives and functions

- Design, implement and supervise the processes of SGF GLOBAL's Personal Data Protection Management System.

- Supervise the register of personal data processing of the company.
- Inform and advise on data protection obligations.
- Supervise compliance with regulations.
- Advise on the impact assessment related to the protection of personal data.
- Supervise compliance and implementation of the identified risk mitigation measures.
- Supervise the investigation of personal data protection incidents.

7.2.2 Governance and organization of the Data Protection Committee

The Personal Data Protection Committee is made up of the following roles and operational teams, where the representation of those areas that have a greater impact on its management and treatment has been sought:

- Representative within all company departments in each country where we operate.

7.3 Roles: Functions and Responsibilities

In the case of SGF GLOBAL, all responsibilities fall on the Management, where the property of the company is located.

SGF GLOBAL must guarantee, at least, the existence of three different figures for each system based on the following responsibilities:

- Responsible for the Information
- Responsible of the service
- Data Protection Officer

The roles and responsibilities are detailed below:

a) Responsible for the Information It has the following functions and responsibilities:
   - Ensure the proper use of the information of its competence and, therefore, its protection.
   - Be ultimately responsible for any error or negligence that leads to an incident of confidentiality or integrity, of the information for which it is responsible.
   - Determine the levels of information security.
   - Formally approve the level of information security.

b) Responsible for the Service It has the following functions and responsibilities:
   - Establish the requirements of the security services that must be guaranteed in the treatment of information, including the requirements of interoperability, accessibility, and availability.
   - Assess the different dimensions of security (availability, confidentiality) for each service contemplated in the risk analysis.

c) Data Protection Delegate Has the following functions and responsibilities:
   - Collaborate in establishing the security requirements that must be guaranteed in the treatment of the information for which it is responsible.
   - Collaborate in the assessment of each information contemplated in the risk analysis of the different security dimensions (availability, confidentiality, integrity, authenticity and traceability).
   - Work in collaboration with the person responsible for Information Security and Information Systems in the maintenance of the systems.

- Ensure the inclusion of security clauses in contracts with third parties and their compliance.
- Inform and advise the person in charge or the person in charge of the treatment and the employees who deal with the treatment of the obligations regarding the protection of personal data.
- Collaborate in the Supervision of the assignment of responsibilities.
- Supervise the awareness and training of the personnel involved in the treatment operations.
- Supervise the corresponding audits.
- Offer the advice that is requested about the impact assessment related to data protection.
- Collaborate in the Supervision of the assignment of responsibilities.
- Supervise the awareness and training of the personnel involved in the treatment operations.

7.4 Information Security Policy

The mission of the Cybersecurity Committee will be the annual review of this Information Security Policy and the proposal for its revision or maintenance. The Policy will be approved by the Management and disseminated so that all affected parties are aware of it. And will report to the Safety Committee.

- The Director of the IT Systems department (CIO) may create and designate specific roles, for Corporation or Delivery, such as:
- The System Manager
- The Head of Administration
- The Systems Security Manager
- The Head of the Corporate Cybersecurity Office

Once appointed, they must be transferred to the General Directorate through the functional structures.

VII. Personal data

It is about guaranteeing and protecting, as regards the processing of personal data, public freedoms and fundamental rights of natural persons, and especially their honor, intimacy and personal and family privacy, and is applicable to data of a personal nature registered both electronically and on paper.

All SGF GLOBAL information systems will adjust to the security levels required by the regulations for the nature and purpose of the personal data collected for processing.

To guarantee said protection, the security measures that correspond to the requirements set forth in the applicable legislation have been adopted.

Any internal or external user who, by virtue of their professional activity, could have access to personal data, is obliged to keep them secret, a duty that will be maintained indefinitely, even beyond the employment or professional relationship with SGF GLOBAL.

VIII. Risk management

All systems subject to this Policy must carry out a risk analysis, evaluating the threats and risks to which they are exposed.

This analysis will be reviewed:

- Regularly, at least once a year.
- When the information handled changes.
- When the services provided change.
- When a serious security incident occurs.
- When serious vulnerabilities are reported.

For the harmonization of risk analysis, the Corporate Cybersecurity Committee will establish a reference assessment for the different types of information handled and the different services provided. The Corporate Cybersecurity Committee will boost the availability of resources to meet the security needs of the different systems, promoting horizontal investments.

Risk management will be documented in the Risk Analysis and Management report.

IX. Risk Management

All systems subject to this Policy must perform a risk analysis, evaluating the threats and risks to which they are exposed.

This analysis will be reviewed:

- Regularly, at least once a year.
- When the information handled changes.
- When the services provided change.
- When a serious security incident occurs.
- When serious vulnerabilities are reported.

For the harmonization of risk analysis, the Corporate Cybersecurity Committee will establish a reference assessment for the different types of information handled and the different services provided. The Corporate Cybersecurity Committee will boost the availability of resources to meet the security needs of the different systems, promoting horizontal investments.

Risk management will be documented in the Risk Analysis and Management report.

X. Development of the Information Security Policy

10.1 Policy for the Use of Information Systems

The "Internal Policy for the Use of Information Systems" is published on the SGF GLOBAL intranet, which aims to regulate the use of information systems owned by SGF GLOBAL made available to its workers and users, as well as to guarantee the security, legality, performance, integrity and privacy of the information, preserve the privacy and security of the personnel and in general, guarantee the effective fulfillment of the activities and other tasks that emanate from the strictly work environment.

It is not considered acceptable:

- The creation, use or transmission of material in violation of data protection or intellectual property laws.
- Install, modify or change the configuration of the software systems (only the administrators of the equipment are authorized to do so).

- Use of the Internet for personal purposes (including personal web-based email) will be limited to authorized break times.
- Any personal electronic transaction that is carried out will be under the responsibility of the user.
- Deliberately facilitating access to facilities or services for unauthorized persons.
- Willfully wasting network resources.
- Corrupt or destroy data of other users or violate their privacy intentionally.
- Intentionally introducing viruses or other forms of malicious software. Before using any information storage, it must be verified that it is free of viruses or the like.
- Disclosing passwords and means of access voluntarily.
- Use the equipment for personal gain.
- The creation, use or transmission of offensive, obscene material or that may cause annoyance or offense.
- Send very large e-mails or to a very large group of people (which can saturate the communications).
- Do not verify that the emails are free of virus.

10.2 Security of Human Resources Management

Security related to personnel is essential to reduce the risks of human error, theft, fraud or misuse of facilities and services.

The signing of a confidentiality agreement will be required for all employees to prevent the disclosure of confidential information.

All security policies and procedures must be communicated regularly to all workers and third party users, if applicable.

When the employment or contractual relationship with employees or external personnel is terminated, their access permits to the facilities and information will be withdrawn and they will be asked to return any type of information or equipment that has been delivered to them to carry out the work. .

10.3 Physical and Environmental Security

For a logical security to be effective, it is essential that the facilities maintain correct physical security to prevent unauthorized access, as well as any other type of damage or external interference.

10.3.1 Safe Areas

SGF GLOBAL will take the necessary precautions so that only authorized persons have access to the facilities.

All SGF GLOBAL facilities have the necessary physical barriers to ensure the resources they house and the accompaniment of staff during their stay at the facilities.

10.3.2 Equipment Safety

Computer equipment is an important asset on which the continuity of activities depends, so they will be adequately and effectively protected.

SGF GLOBAL IT equipment is protected against possible power failures (laptop with battery, UPS, etc.)

The equipment must be properly maintained to guarantee its correct functioning and its perfect state of form so that it maintains the confidentiality, integrity and, above all, the availability of the information. To do this, they must undergo the reviews recommended by the supplier. Only duly authorized personnel may access the equipment to proceed with its repair. It will also be necessary to adopt the necessary precautionary measures in case the equipment must leave the facilities for maintenance.

10.4 Communications and Operations Management

10.4.1 Operating Procedures and Responsibilities

SGF GLOBAL will control access to services on internal and external networks and will ensure that users do not put these services at risk. To do this, it must establish the appropriate interfaces between the SGF GLOBAL network and other networks, the appropriate authentication mechanisms for users and equipment, and the accesses for each user of the information system.

To prevent malicious use of the network, there will be mechanisms to limit the network services that can be accessed, authorization procedures to establish who can access which network resources, and management controls to protect network access.

All employees authorized to handle automated information must be registered as domain users. Each time they access the information system, they must be validated with their username, which will be unique and non-transferable, and their personal password.

This password will periodically expire.

To ensure the correct and safe operation of the information systems, the operating procedures will be duly documented and will be implemented in accordance with these procedures. These procedures will be reviewed and suitably modified when there are significant changes in the equipment or software that require it.

In some cases it will be necessary for different areas to be logically separated from the rest to prevent unauthorized access.

The installation of other software that is not permitted and necessary for the development of the work by SGF GLOBAL personnel is totally prohibited.

All software acquired by the organization, whether by purchase, donation or assignment, is the property of the institution and will maintain the rights that the intellectual property law confers on it, monitoring the different types of licenses.

Any software that needs to be installed to work on the network must be evaluated and authorized by the Cybersecurity Committee.

The System Administrator will install the appropriate computer tools to protect systems against viruses, worms, Trojans, etc. and users must follow the guidelines given to them to protect the equipment, applications and information with which they work.

10.4.2 Backups

The data must be stored according to the rules established in the Information Systems Use Policy, to ensure their availability.

10.4.3 Network Security Management

The network elements (switch, router ... etc.) will remain out of the access of unauthorized personnel to avoid malicious use that could jeopardize the security of the system.

There will be a graphical management of the network so that its maintenance can be more comfortable.

10.5 Media Management

Users will apply the same security measures to media containing sensitive information as to the files from which they have been extracted.

10.5.1 Exchange of Information

Procedures will be established to protect the information exchanged through any means of communication (electronic, verbal, fax, etc.).

10.5.2 Monitoring

As deemed necessary, the necessary mechanisms will be established to detect unauthorized information processing activities. This will involve performing tasks to carry out controls and inspections of the system records and activities to test the efficiency of data security and data integrity procedures, to ensure compliance with established policy and operating procedures, as well as to recommend any changes deemed necessary.

10.6 Access Control

10.6.1 Service Requirements for Access Control

The information must be protected against unauthorized access. The Service Manager will define the needs for access to information at two levels, for the set of areas and for each user within the set. Access will only be provided to the information necessary for the work to be carried out.

10.6.2 User Access Management

The system administrator is responsible for providing users with access to computing resources, as well as specialized logical access to resources (servers, routers, databases, etc.) connected to the network.

10.6.3 Network Access Control

Staff workstations should be clear of papers and other information storage media to reduce the risks of unauthorized and other access.

Access to the network, systems, applications, or information will not be allowed to any user who is not formally authorized to do so.

In the case of service providers or external entities, who need to access them for a justified reason, they are required to sign confidentiality agreements with SGF GLOBAL and convey the security policy, rules and procedures that they must adopt, to maintain the same. level of security than if they were employees of the organization itself.

The use of free or third-party VPN services to access company information systems is not recommended.

Access to information systems from anonymization networks (TOR, I2P, etc.) and other services commonly used to carry out illegal actions and whose purpose is to hide the real origin of the connections will be restricted, whenever possible.

Each user must be associated with a profile, according to the tasks performed in the organization, defined by their direct manager.

Each of these profiles will have certain permissions and will be restricted from accessing information and systems that are not necessary for the skills of their work.