VGPSI – OVERVIEW OF INFORMATION SECURITY PROCESSES

Classification: Open

Version 1.3

Elaboration:	Approval:	Creation date:	Validity:
Information Security	IS Manager	11/03/2022	11/03/2026

SUMMARY

1. INTRODUCTION

1.1. Objective

To provide customers and partners with an overview of information security processes.

1.2. Responsible

The Information Security department is responsible for updating this document.

2. Standards

2.1. Information Security Incident Handling

NSI007 - INFORMATION SECURITY INCIDENT HANDLING STANDARD

Responsibilities and procedures - Defines guidelines to ensure that management responsibilities and procedures are in place to ensure rapid, effective and orderly responses to information security incidents. It establishes responsibilities and procedures for identifying and recording personal data breaches as part of the global information security incident management process.

Notification of information security events - Defines guidelines to ensure that information security events are reported through the appropriate management channels as quickly as possible.

Evaluating and deciding on information security events - Ensuring that information security events are properly evaluated, validating whether they are classified as information security incidents.

Reporting information security weaknesses - Defines guidelines to ensure that both employees and other external parties who use the organization's information systems and services are properly instructed to record and report any suspected or observed information security weaknesses in the systems or services.

Response to information security incidents - Defines guidelines to ensure that documented procedures are followed so that information security incidents can be properly reported.

Learning from information security incidents - We have defined an internal process to ensure that the knowledge gained during the resolution of information security incidents is used to reduce the likelihood or impact of future incidents.

Contact with authorities - Contact with authorities may be necessary during the handling of information security incidents, in addition to support in dealing with legal issues, which is why LG lugar de gente implements procedures that specify when and which authorities (e.g., ANPD, legal obligations, fire department, inspection authorities, regulatory bodies) will be contacted and how identified information security and privacy incidents will be reported in a timely manner (e.g., in the event of suspicion that the law has been violated).

2.2. Risk Analysis, Assessment and Treatment

NSI003 - RISK ANALYSIS, ASSESSMENT AND TREATMENT STANDARD

Information Security Risk Assessment - LG Lugar de Gente defines and applies a risk assessment process that establishes and maintains criteria that include risk acceptance, criteria for performing risk assessments, and ensures that ongoing information security risk assessments produce comparable, valid, and consistent results. The aim is to ensure that information security risks are identified by applying the assessment process to identify the risks associated with the loss of confidentiality, integrity and availability of information within the scope of the information security management system.

Information security risk treatment - We define and apply a risk treatment process to appropriately select risk treatment options, considering the results of the risk assessment. It determines all the controls that are necessary to implement the chosen risk treatment options. This is dealt with through action plans to mitigate information security risks. In this process, the approval of those responsible and the acceptance of residual risks are obtained.

2.3. Access control

NSI006 - ACCESS CONTROL STANDARD

Access control policy - Defines guidelines for managing access to information assets by employees, service providers, partners and suppliers. These guidelines aim to limit access to information and information processing resources and ensure that physical and logical access is granted only to authorized persons, reducing the related Information Security risks.

Responsibilities for termination or change of contract - Ensure that all the organization's information resources and assets are withdrawn or returned to the organization, reducing the risk of personal data breaches and Information Security incidents.

Withdrawal or adjustment of access rights - Defines guidelines to ensure that users' access is adjusted or withdrawn when it is no longer necessary, preventing undue access to the organization's resources.

Restricting access to information - Ensuring that users only have access to the resources they need to carry out their activities, avoiding undue or insufficient access.

Access to networks and network services - Defines guidelines to ensure that access to the corporate network is carried out only by authorized persons, reducing the related Information Security risks.

Provision for user access - Defines guidelines to ensure that users only receive access to the resources they need to carry out their activities, avoiding undue or insufficient access. To this end, we keep an accurate and up-to-date record of the user profiles created for users who have been authorized to access the information system and the personal data contained therein.

Management of privileged access rights - Defines guidelines to ensure that privileged access is granted exclusively to users who need this type of resource to carry out their activities, preventing undue access.

NSI005 - REMOTE ACCESS STANDARD

Remote working - Contains guidelines for granting remote access to employees and service providers to address risks related to remote working. To do this, we use mobile devices with special care to ensure that business information and personal data are not compromised.

Policy for the use of mobile devices - Defines rules to ensure that the use of mobile devices does not imply a violation of the Information Security rules defined by the company. Ensures that the use of mobile devices does not lead to the compromise of personal data.

2.4. Monitoring information assets and services

NSI013 - MONITORING INFORMATION ASSETS AND SERVICES STANDARD

Event records - LG lugar de gente establishes a process to critically analyze event records (logs) using continuous automated alert and monitoring processes, or also manually, where such critical analysis is performed at a specified and documented periodicity, with a view to identifying irregularities and proposing remediation efforts. Ensure that information security records and events are produced, maintained and critically analyzed at regular intervals.

Capacity management - Defines rules to ensure that resource utilization within the scope of the ISMS is monitored, adjusted and projections made for future capacity needs to ensure the required system performance.

NSI017 - SGSI AND SGPI INDICATORS STANDARD

Monitoring, measurement, analysis and evaluation - Contains guidelines to ensure the monitoring of SGSI and SGPI indicators, aiming at the continuous improvement of the Integrated Information Security and Privacy Management System (SGSI and SGPI), based on the ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO/IEC 27018:2021 and ISO/IEC 27017:2016, with indicators and metrics to monitor the SGSI and SGPI throughout the PDCA cycle.

2.5. Clean Table and Acceptable Use of Assets

NSI008 - CLEAN DESK AND ACCEPTABLE ASSET USE STANDARD

Clean desk and clean screen policy - Defines guidelines for the acceptable use of your information assets. These guidelines aim to ensure that information, both on physical media and stored on electronic media, is not accessed in an unauthorized way.

Physical and environmental security - Ensuring the protection of critical areas of the organization, within the scope of the SGSI. Ensuring that deliveries or shipments are carried out in such a way as not to incur Information Security risks.

Return of assets - Defines guidelines to ensure that all employees and external parties return all assets of the organization that are in their possession, after the termination of their activities, the contract or agreement.

Removable media management - Defines procedures for managing removable media, according to the classification scheme adopted by the organization. Use removable physical media and/or devices that allow encryption when storing personal data.

Equipment maintenance - Ensuring correct maintenance to guarantee the availability and integrity of the organization's equipment.

Security of equipment and assets outside the organization's premises - Defines rules to ensure adequate levels of protection for assets operating outside the company's premises, considering the different risks arising from working outside the organization's premises.

2.6. Information Handling and Classification

NSI004 - INFORMATION HANDLING AND CLASSIFICATION STANDARD

Information classification - Ensuring that information receives an appropriate level of protection, according to its importance to the organization. The aim is to ensure that all information assets within the scope of the ISMS and IMMS are properly classified, so that they can receive Information Security and privacy controls compatible with their classification level.

Labels and information handling - These state the rules for implementing and maintaining an appropriate set of procedures for labeling and handling information in accordance with the information classification scheme adopted by LG lugar de gente. Within these procedures, personal data is explicitly considered as part of the organization's information classification scheme. This control aims to ensure that information assets within the scope of the ISMS have their classification level easily identified, so that information can be handled within the Information Security rules defined by the organization.

Reuse and/or safe disposal of equipment - Defines a rule to ensure that the reuse or disposal of equipment does not lead to Information Security risks such as unauthorized access or loss of information.

Policies and procedures for information transfer - Defines guidelines to ensure the protection of information during transfer using all types of communication resources.

Information transfer agreements - We have defined rules to ensure that agreements exist for the secure transfer of business information between the organization and external parties.

2.7. Development and design of secure systems

NSI014 - SECURE DEVELOPMENT STANDARD AND INFORMATION SECURITY AND PDP REQUIREMENTS

Development, test, homologation and production environments– Establishes guidelines for separating and protecting environments, prohibiting the use of real data in tests and requiring access control, logging and log maintenance.

Requirements for secure development – Defines mandatory practices for authentication, authorization, session management, error handling, file uploads and information reliability, with a focus on security right from the system's design.

Personal data protection – Establishes guidelines based on Privacy by Design and Privacy by Default, including principles such as minimization, use limitation, consent, accuracy, security and accountability, applicable to all systems that process personal data.

Outsourced development – Defines criteria for contracting third parties, including control of intellectual property, use of LG tools, compliance with internal policies and carrying out acceptance tests.

Security testing and validation – Requires security testing before going into production, code reviews, vulnerability analysis and documentation of the results, with a focus on confidentiality, integrity and availability.

Logging of events and logs – Establishes rules for generating, storing and analyzing logs, with a focus on traceability, access control and prohibiting the storage of sensitive data.

2.8. Use of e-mail

NSI009 - ELECTRONIC MAIL USE STANDARD

Electronic messages - contains organizational guidelines for the use of e-mail under the "@lg.com.br" domain, allowing only internal employees and third parties to accordance with the third-party contracting process. It establishes technical cybersecurity measures to ensure that information that travels in electronic messages is adequately protected.

2.9. Internet access and social media behavior

NSI012 - INTERNET ACCESS, SOCIAL MEDIA BEHAVIOR AND ARTIFICIAL INTELLIGENCE USE STANDARD

It contains guidelines for the safe use of internet access provided by LG lugar de gente, the behavior of employees, suppliers and third-party contractors on social media and networks and for the use of artificial intelligence.

2.10. Cloud Security and Privacy

NSI019 - CLOUD SECURITY AND PRIVACY STANDARD

Cloud Service - Contains the practices for contracting, managing and using cloud computing services in LG lugar de gente's corporate environment, describing the controls necessary for their proper use.

Cloud Security and Privacy - Contains requirements and criteria to guarantee security and privacy in the provision and contracting of cloud services.

Compliance - Defines responsibilities for the Information Security and Legal areas to assess whether legal compliance regulations to which the company is subject will be impacted using cloud services. It also ensures that all cloud platforms, infrastructure and service providers comply with data protection laws and regulations, as well as the standards and policies adopted by LG lugar de gente.

Business continuity - Establishes criteria to ensure that potential failures do not impact on the continuity of business in the cloud.

2.11. Other Standards

There are other standards that represent additional administrative controls and help maintain the security of LG Lugar de Gente's information assets. The standards are based on the best security practices and comply with ISO 27001:2013:

- Supplier Management
- Responsibilities of the CGSI
- Information Security Responsibilities
- Ethical Conduct of Employees
- Cryptographic Key Management
- SGSI and SGPI Internal Audit
- Protection against malicious code
- Organization of Information Security Concept and PDP
- Asset Configuration