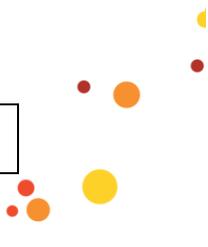


# **VGPSI - VISÃO GERAL DOS PROCESSOS DE SEGURANÇA DA INFORMAÇÃO**

**Classificação:** Pública

Versão 1.1

|                                   |                             |                             |                         |
|-----------------------------------|-----------------------------|-----------------------------|-------------------------|
| Elaboração:<br>Seg. da Informação | Aprovação:<br>Gerente de SI | Data criação:<br>03/11/2022 | Validade:<br>03/11/2024 |
|-----------------------------------|-----------------------------|-----------------------------|-------------------------|



# SUMÁRIO

|   |   |
|---|---|
| <b>1. INTRODUÇÃO</b> .....  | 3 |
| 1.1. <b>Objetivo</b> .....  | 3 |
| 1.2. <b>Responsável</b> .....   | 3 |
| <b>2. Normatizações</b> .....   | 3 |
| 2.1. <b>Tratamento de Incidentes de Segurança da Informação</b> ..... | 3 |
| 2.2. <b>Análise, Avaliação e Tratamento de Riscos</b> .....           | 4 |
| 2.3. <b>Controle de Acesso</b> .....                                  | 4 |
| 2.4. <b>Monitoramento de ativos e serviços da informação</b> .....    | 5 |
| 2.5. <b>Mesa Limpa e Uso Aceitável de Ativos</b> .....                | 6 |
| 2.6. <b>Manuseio e Classificação da Informação</b> .....              | 6 |
| 2.7. <b>Desenvolvimento e projetos de sistemas seguros</b> .....      | 7 |
| 2.8. <b>Uso do correio eletrônico</b> .....                           | 7 |
| 2.9. <b>Acesso à Internet e Comportamento em mídias sociais</b> ..... | 8 |
| 2.10. <b>Outras Normas</b> .....                                      | 8 |

# 1. INTRODUÇÃO

## 1.1. Objetivo

Informar aos clientes e parceiros a visão geral dos processos de segurança da informação.

## 1.2. Responsável

A área de Segurança da Informação é responsável pela atualização desse documento.

# 2. Normatizações

## 2.1. Tratamento de Incidentes de Segurança da Informação

NSI007 - NORMA DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

**Responsabilidades e procedimentos** – Define diretrizes para garantir que existam responsabilidades e procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação. Estabelece responsabilidades e procedimentos para a identificação e registro de violações de dados pessoais, como parte do processo de gestão de incidentes de segurança da informação global.

**Notificação de eventos de segurança da informação** – Define diretrizes para garantir que eventos de segurança da informação sejam relatados através dos canais apropriados da direção, o mais rapidamente possível.

**Avaliação e decisão dos eventos de segurança da informação** - Garantir que eventos de segurança da informação sejam adequadamente avaliados, validando se estes são classificados como incidentes de segurança da informação.

**Notificando fragilidades de segurança da informação** – Define diretrizes para garantir que tanto colaboradores, quanto demais partes externas que usam os sistemas e serviços de informação da organização, estejam adequadamente instruídos a registrar e notificar quaisquer fragilidades de segurança da informação, suspeita ou observada, nos sistemas ou serviços.

**Resposta aos incidentes de segurança da informação** – Define diretrizes para garantir que os procedimentos documentados sejam seguidos para que incidentes de segurança da informação possam ser adequadamente reportados.

**Aprendendo com os incidentes de segurança da informação** – Definimos um processo interno para garantir que os conhecimentos obtidos durante a resolução de incidentes de segurança da informação sejam utilizados para reduzir a probabilidade ou o impacto de incidentes futuros.

**Contato com autoridades** - O contato com autoridades pode ser necessário durante tratamento de incidentes de segurança da informação, além de apoio no atendimento a questões legais, por isso a LG lugar de gente Implementa procedimentos que especificam quando e quais autoridades (por exemplo, ANPD, obrigações legais, corpo de bombeiros,

autoridades fiscalizadoras, organismos regulatórios) serão contatadas e como os incidentes de segurança e privacidade da informação identificados serão reportados em tempo hábil (por exemplo, no caso de suspeita de que a lei foi violada).

## 2.2. Análise, Avaliação e Tratamento de Riscos

### NSI003 - NORMA DE ANÁLISE, AVALIAÇÃO E TRATAMENTO DE RISCOS

**Avaliação de riscos de segurança da informação** - a LG lugar de gente define e aplica um processo de avaliação de riscos que estabelece e mantém critérios que incluem a aceitação do risco, os critérios para o desempenho das avaliações dos riscos e assegure que as contínuas avaliações de riscos de segurança da informação produzam resultados comparáveis, válidos e consistentes. Com isso visa garantir que se identifique os riscos de segurança da informação aplicando o processo de avaliação para identificar os riscos associados com a perda de confidencialidade, integridade e disponibilidade da informação dentro do escopo do sistema de gestão da segurança da informação.

**Tratamento de riscos de segurança da informação** - Definimos e aplicamos um processo de tratamento dos riscos para selecionar, de forma apropriada, as opções de tratamento dos riscos, levando em consideração os resultados da avaliação do risco. Determina todos os controles que são necessários para implementar as opções escolhidas do tratamento do risco. O tratamento é realizado através de planos de ação para mitigação dos riscos de segurança da informação. Neste processo se obtém a aprovação dos responsáveis e a aceitação dos riscos residuais.

## 2.3. Controle de Acesso

### NSI006 - NORMA DE CONTROLE DE ACESSO

**Política de controle de acesso** – Define diretrizes para gestão de acesso dos colaboradores, prestadores de serviços, parceiros e fornecedores aos ativos de informação. Estas diretrizes visam limitar o acesso à informação e aos recursos de processamento da informação e garantir que acessos, físicos e lógicos, sejam concedidos apenas a pessoas autorizadas, reduzindo os riscos de Segurança da Informação relacionados.

**Responsabilidades pelo encerramento ou mudança da contratação** - Garantir que o todos os recursos e ativos de informação da organização sejam retirados ou devolvidos para a organização, reduzindo o risco de violações de dados pessoais e incidentes de Segurança da Informação.

**Retirada ou ajuste dos direitos de acesso** – Define diretrizes para garantir que o acesso dos usuários seja ajustado ou retirado quando não for mais necessário, evitando acessos indevidos a recursos da organização.

**Restrição de acesso à informação** - Garantir que usuários tenham acesso apenas aos recursos necessários ao desempenho de suas atividades, evitando acessos indevidos ou insuficientes.

**Acesso às redes e aos serviços de rede** – Define diretrizes para garantir que o acesso à rede corporativa seja realizado apenas por pessoas autorizadas, reduzindo os riscos de Segurança da Informação relacionados.

**Provisionamento para acesso de usuário** – Define diretrizes para garantir que usuários recebam acesso apenas aos recursos necessários ao desempenho de suas atividades, evitando acessos indevidos ou insuficientes. Para isso mantemos um registro preciso e atualizado dos perfis dos usuários criados para os usuários que tenham sido autorizados a acessar o sistema de informação e os dados pessoais neles contidos.

**Gerenciamento de direitos de acesso privilegiado** – Define diretrizes para garantir que acesso privilegiado seja concedido exclusivamente a usuários que necessitam deste tipo de recurso para o desempenho de suas atividades, evitando acessos indevidos.

#### NSI005 - NORMA DE ACESSO REMOTO

**Trabalho remoto** - Contém diretrizes para concessão de acesso remoto para os colaboradores e prestadores de serviços com objetivo de tratar riscos relacionados ao trabalho remoto. Para isso utilizamos dispositivos móveis com cuidados especiais para assegurar que as informações do negócio e dados pessoais não sejam comprometidas.

**Política para o uso de dispositivo móvel** – Define regras para garantir que o uso de dispositivos móveis não implique em violação das regras de Segurança da Informação definidas pela empresa. Assegura que o uso de dispositivos móveis não conduza a um comprometimento de dado pessoal.

## 2.4. Monitoramento de ativos e serviços da informação

#### NSI013 – NORMA DE MONITORAMENTO DE ATIVOS E SERVIÇOS DE INFORMAÇÃO

**Registros de eventos** – A LG lugar de gente estabelece um processo para analisar criticamente os registros de eventos (logs) usando processos contínuos de alerta e monitoramento automatizados, ou também manualmente, onde que tal análise crítica seja desempenhada em uma periodicidade especificada e documentada, visando identificar irregularidades e propor esforços de remediação. Garantir que registros e eventos de segurança da informação são produzidos, mantidos e analisados criticamente, a intervalos regulares.

**Gestão de capacidade** – Define regras para garantir que a utilização dos recursos dentro do escopo do SGSI é monitorada, ajustada e as projeções devem ser feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema.

#### NSI017 – NORMA DE INDICADORES DO SGSI E SGPI

**Monitoramento, medição, análise e avaliação** - contém diretrizes para garantir o monitoramento de indicadores do SGSI e SGPI, visando a melhoria contínua do Sistema de Gestão Integrado de Segurança e Privacidade da Informação (SGSI e SGPI), com base na norma ISO/IEC 27001:2013 ISO/IEC 27701:2019, possuindo os indicadores e métricas para monitorar o SGSI e SGPI durante todo o ciclo PDCA.

## 2.5. Mesa Limpa e Uso Aceitável de Ativos

### NSI008 - NORMA DE MESA LIMPA E USO ACEITÁVEL DE ATIVOS

**Política de mesa limpa e tela limpa** - Define diretrizes para o uso aceitável de seus ativos da informação. Estas diretrizes visam garantir que informações, tanto em meios físicos quanto armazenadas em meios eletrônicos, não sejam acessadas de forma não autorizada.

**Segurança física e do ambiente** - Garantir a proteção de áreas críticas da organização, dentro do escopo do SGSI. Garantir que a realização de entregas ou carregamentos seja realizada de forma a não incorrer em riscos de Segurança da Informação.

**Devolução de ativos** – Define diretrizes para garantir que todos os funcionários e partes externas devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.

**Gerenciamento de mídias removíveis** - Define procedimentos para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização. Usar mídias físicas removíveis e/ou dispositivos que permitam a criptografia, quando do armazenamento de dado pessoal.

**Manutenção dos equipamentos** - Garantir a manutenção correta para assegurar a disponibilidade e integridade dos equipamentos da organização.

**Segurança de equipamentos e ativos fora das dependências da organização** – Define regras para garantir níveis adequados de proteção para ativos que operam fora do local da empresa, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.

## 2.6. Manuseio e Classificação da Informação

### NSI004 - NORMA DE MANUSEIO E CLASSIFICAÇÃO DA INFORMAÇÃO

**Classificação da informação** - Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização. O objetivo é garantir que todos os ativos de informação dentro do escopo do SGSI e do SGPI estejam adequadamente classificados, de forma que possam receber controles de Segurança e privacidade da Informação compatíveis com o seu nível de classificação.

**Rótulos e tratamento da informação** – Declara as regras para implementação e manutenção de um conjunto apropriado de procedimentos para rotular e tratar a informação de acordo com o esquema de classificação da informação adotado pela LG lugar de gente. Dentro desses procedimentos é considerado explicitamente o dado pessoal como parte do esquema de classificação da informação da organização. Este controle visa garantir que ativos de informação no escopo do SGSI tenham seu nível de classificação facilmente identificado, de forma que o tratamento da informação possa ser realizado dentro das regras de Segurança da Informação definidas pela organização.

**Reutilização e ou descarte seguro de equipamentos** – Define regra para garantir que a reutilização ou descarte de equipamentos não implique em riscos de Segurança da Informação como acesso não autorizado ou perda de informação.

**Políticas e procedimentos para transferência de informações** – Define diretrizes para garantir a proteção de informações durante a transferência por meio do uso de todos os tipos de recursos de comunicação.

**Acordos para transferência de informações** – Definimos regras para garantir a existência de acordos para transferência segura de informações do negócio entre a organização e partes externas.

## 2.7. Desenvolvimento e projetos de sistemas seguros

NSI014 - NORMA DE REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PDP

**Procedimentos seguros de entrada no sistema (log-on)** – Define os requisitos para desenvolvimento seguro das ofertas da LG lugar de gente, incluindo diretrizes de Privacy by Design e Privacy by Default com base nas obrigações dos titulares de dados pessoais e/ou qualquer legislação aplicável e/ou regulamentação e os tipos de tratamentos realizados pela organização. Essas regras são aplicadas também para aquisição de novos sistemas e serviços de TI.

**Sistema de gerenciamento de senha** – Define as regras para garantir o uso de senhas com qualidade/complexidade compatível aos sistemas, aplicações e demais ativos de informação.

**Criptografia** – Define os requisitos de forma a garantir que os controles criptográficos necessários sejam aplicados, reduzindo os riscos à Segurança e Privacidade da Informação associados a desenvolvimento e contratação de softwares de terceiros.

**Segurança da informação no gerenciamento de projetos** – Define os requisitos de Segurança da Informação e Privacidade no gerenciamento de projetos garantindo que esses requisitos sejam seguidos durante projetos executados pela LG lugar de gente.

**Registro de eventos** – Define os requisitos para garantir que registros e eventos de Segurança da Informação são produzidos, mantidos e analisados criticamente, a intervalos regulares.

**Políticas e procedimentos para transferência de informações** – Define as regras para garantir a proteção de informações durante a transferência dos dados.

## 2.8. Uso de correio eletrônico

NSI009 - NORMA DE USO DE CORREIO ELETRÔNICO

**Mensagens eletrônicas** - contém diretrizes organizacionais para uso do e-mail sob o domínio "@lg.com.br", permitindo apenas para colaboradores internos e terceiros de acordo com o processo de contratação de terceiros. Estabelece medidas técnicas de segurança cibernética visando garantir que informações que trafegam em mensagens eletrônicas são adequadamente protegidas.

## 2.9. Acesso à Internet e Comportamento em mídias sociais

### NSI012 - NORMA DE ACESSO À INTERNET, COMPORTAMENTO EM MÍDIAS SOCIAIS E USO DE INTELIGÊNCIA ARTIFICIAL

Contém diretrizes para utilização segura do acesso à internet fornecido pela LG lugar de gente, do comportamento de colaboradores, fornecedores e terceiros contratados em mídias e redes sociais e para o uso de inteligência artificial.

## 2.10. Outras Normas

Existem outras normas que representam controles administrativos adicionais e auxiliam na manutenção da segurança dos ativos de informação da LG Lugar de Gente. As normas são baseadas nas melhores práticas de segurança e atende a ISO 27001:2013:

- Gerenciamento de Fornecedores
- Responsabilidades do CGSI
- Responsabilidades de Segurança da Informação
- Conduta Ética de Colaboradores
- Gerenciamento de Chaves Criptográficas
- Auditoria Interna do SGSI e do SGPI
- Proteção contra Códigos Maliciosos
- Organização de Conceito de Segurança da Informação e PDP