Superlógica

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
PROCEDIMENTO

Versão 2.1
Classificação: Publica

Elaborado por:	Verificado por:	Aprovado por:
Gabriel Donato	Mayara Santos Jean Rodrigues	Jhonatas Faria
Data: 19/12/2022	Data: 30/12/2022	Data: 31/12/2022

Revisão	Descrição	Autor	Data
2.0	Reestruturação	Gabriel Donato	19/12/2022
2.1	Atualização	Mayara Mattos	30/11/2023

1. APRESENTAÇÃO

A Política de Segurança da Informação é o documento que expressa o posicionamento do Grupo Superlógica em relação à proteção das suas informações e dos seus dados.

É dever de todos seguir as orientações contidas neste documento, bem como em todo o conjunto de normas e procedimentos que formam a matéria, para mantermos a elevada confiabilidade e credibilidade de nosso ecossistema e honrarmos nosso compromisso para garantia da confidencialidade, integridade e disponibilidade da informação.

As diretrizes a serem seguidas serão apresentadas neste documento e alegar seu desconhecimento é inescusável.

2. OBJETIVO

Esta Política de Segurança da Informação tem o objetivo de orientar, por meio das suas diretrizes, todas as ações de segurança, para mitigar os riscos, garantindo assim e priorizando os seguintes princípios da Tríade de Segurança:

CONFIDENCIALIDADE: A confidencialidade deverá ser preservada em todos os processos, sustentando sempre a relação com o cliente e de acordo com os casos em que a Confidencialidade possa infringir o estabelecido na LGPD;

INTEGRIDADE: A informação deverá ser íntegra, seu estado, definições e características deverão ser mantidas de acordo com o estabelecido por seu(s) responsável(eis), sem quaisquer alterações indevidas durante seu processamento, armazenamento e distribuição;

DISPONIBILIDADE: A informação deverá estar sempre disponível, considerando o estabelecido em seu contrato ou diretrizes internas, exceto nos casos em que por motivos de força maior ou mediante prévia notificação, esteja indisponível ou seja necessário estar indisponível. A informação poderá estar indisponível nos casos em que a manutenção dos ambientes e ativos seja necessária por motivos de segurança ou para preservar a estrutura de nossos serviços.

Tais princípios são essenciais para a preservação das informações das empresas do Grupo Superlógica.

Adicionalmente, esta Política de Segurança da Informação deve contemplar todos os requisitos do PCI DSS.

3. ABRANGÊNCIA

Este documento se aplica aos procedimentos internos, produtos e serviços oferecidos pela Superlógica e demais empresas que compõem ou que venham compor o Grupo Superlógica.

Estas diretrizes aplicam-se a todos os acionistas, colaboradores, terceiros, fornecedores, prestadores de serviço, parceiros e demais partes relacionadas, que se utilizam dos sistemas de informação do Grupo Superlógica, os quais são também, responsáveis pela segurança dos ativos da empresa, estando cientes de seu compromisso com a proteção e o uso adequado da informação.

É indispensável assegurar que todos, independentemente do seu nível hierárquico, função e ou vínculo contratual, tenham conhecimento desta política, sendo exigido destes o respeito pelos controles de segurança implementados e o cumprimento das diretrizes estabelecidas.

Estas diretrizes também se aplicam tanto para o ambiente informatizado, como para ativos de qualquer natureza que armazene, transmita ou processe informações do Grupo Superlógica.

4. DIRETRIZES

As diretrizes propostas pelos gestores, diretores, por normas internas e pelo Grupo Superlógica deverão estar alinhadas com os princípios que regem a Política de Segurança da Informação e cumprirão um papel incremental. Esta Política está acima de qualquer outra norma de Segurança nos casos em que houverem conflitos.

5. TERMOS E DEFINIÇÕES

PCI/DSS (Payment Card Industry/Data Security Standards) - É uma organização que dita os padrões de Segurança da Informação para ambientes que armazenam, transmitem e processam dados do portador do cartão.

Segurança da Informação - São procedimentos que visam garantir a confidencialidade, integridade e disponibilidade das informações.

Vulnerabilidade - Fragilidade ou fraqueza que podem ser exploradas por ameaças e podem tornar-se um incidente.

LGPD - Lei Geral de Proteção de Dados (Lei nº 13.709/2018), é a legislação brasileira que regula as atividades de tratamento de dados pessoais.

Pivoting - Técnica na qual invasores utilizam de arquivos, rastros e configurações do sistema para comprometer outros sistemas da rede interna.

Disaster Recovery - Recuperação de Desastres consiste em uma série de práticas que visa amenizar os impactos sobre incidentes.

Pentest - Testes de intrusão em que hackers éticos buscam adquirir acessos aos sistemas e enumerar as falhas de segurança, a forma como atacantes reais poderiam obter acessos e os desdobramentos dessas invasões.

Firewall - Serviço de monitoramento do tráfego de entrada e saída da rede, para prevenção contra invasões e tráfegos indesejados.

6. ATRIBUIÇÕES E RESPONSABILIDADES

O time de **SEGURANÇA DA INFORMAÇÃO** deverá:

- Promover um ambiente seguro;
- Ser agente facilitador para a implantação dos controles descritos nesta Política, nas normas ou qualquer outra documentação técnica desenvolvida na Superlogica;
- Submeter à Direção da Superlógica quaisquer solicitações que requeiram investimentos financeiros;
- Analisar os casos de descumprimento desta Política e Normas de Segurança da Informação, encaminhando-os para a Diretoria, quando for necessário;
- Propor melhorias e aprovar as Normas de Segurança da Informação e Privacidade;
- Realizar / atualizar treinamentos internos assim como programas de conscientização de Segurança da Informação.

7. RESPONSABILIDADES SOBRE A INFORMAÇÃO

A responsabilidade pela segurança das informações é dada a todos os envolvidos com as operações da Superlógica e todos possuem um papel fundamental na garantia dela.

A propriedade sobre a informação é da Superlógica e deverá ser preservada pelos colaboradores durante o exercício de suas atividades, sendo a propriedade revogada apenas nos casos em que operarmos sob as limitações da LGPD e outras bases legais.

8. BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

Todos os colaboradores deverão estar de acordo com as boas práticas de segurança da informação, que serão exercidas diariamente. Essas práticas são de extrema importância para construirmos um ambiente seguro para os clientes e colaboradores.

Os materiais de boas práticas de segurança da informação estarão disponíveis em nossas ferramentas internas, disponibilizadas durante o Onboarding e disponíveis a qualquer momento, mediante solicitação ao Time de Segurança da Informação.

9. RESPONSABILIDADE DE TERCEIROS

Todos os terceiros (fornecedores, prestadores de serviços, parceiros e pesquisadores de segurança) deverão estar de acordo com esta política de segurança, preservando durante todas as suas atividades os princípios da Segurança da Informação, não excedendo quaisquer limites.

Terceiros deverão operar somente sobre os dados em que forem autorizados e nos casos que motivados por erro humano, tecnológico ou a fim de testar os níveis de segurança implementados, se depararem com dados sensíveis de operação e ou pessoais, deverão reportar o ocorrido imediatamente para nosso canal em: seguranca@superlogica.com, o qual deverá ter uma resposta prévia em até dois dias úteis após seu recebimento.

Todo e qualquer acesso por terceiros em escopo não autorizado poderá sofrer sanções administrativas e legais.

10. RESPOSTA A INCIDENTES

Os incidentes de segurança da informação da Superlógica são monitorados e tratados visando garantir a disponibilidade, integridade e confidencialidade da informação.

As respostas aos incidentes deverão ser conduzidas conforme norma interna a ser observada por todos os colaboradores.

11. POLÍTICA DE PRIVACIDADE

A Política de Privacidade é o documento que dispõe sobre as normas e a forma como fazemos o tratamento dos dados de clientes. Nos casos ou incidentes sobre privacidade dos dados, a Política de Privacidade sobresairá sobre a Política de Segurança da Informação para dispor sobre os deveres e papéis dos responsáveis.
A Política de Privacidade pode ser acessada em: transparencia.superlogica.com.

12. MONITORAMENTO DE AMBIENTES

O monitoramento dos ambientes da Superlógica deverá ser realizado diariamente, em ambientes de produção, ambientes de testes, nas redes e nos demais ativos.

O objetivo deverá ser a observação de infringência dos padrões de segurança, a exposição de *endpoints*, de informações sensíveis de operações e de clientes, e principalmente a observação de indícios de uma invasão ou ataque.

13. BACKUPS

Os ativos da Superlógica deverão ter seus backups realizados frequentemente. A frequência dos backups deverá ser calculada com base no risco em potencial e na importância do ativo.

Os backups deverão ter rotinas bem definidas e documentadas, de acordo com a frequência estabelecida, devendo ser agendado para que não haja instabilidades nos sistemas em Produção. O local de armazenamento dos backups deverá ser externo à rede original, sem que haja qualquer possibilidade de peering ou pivoting por parte de possíveis atacantes e todo o processo de restauração deverá ser documentado.

Os backups deverão ser testados para garantir a integridade dos dados e serem refeitos caso necessário. Os testes de backups deverão ser realizados semestralmente, ou a cada grande atualização dos sistemas e ativos.

14. DISASTER RECOVERY

Os produtos do Grupo Superlógica deverão possuir planos de Disaster Recovery, a fim de manter a continuidade dos negócios e prevenir danos aos produtos e clientes.

Os planos de Disaster Recovery devem ser documentados e acessíveis, para que todas as áreas envolvidas tenham bem estabelecido quais passos devem ser seguidos no restabelecimento dos serviços e produtos.

15. PENTESTS INTERNOS E EXTERNOS

Os Pentests deverão ser realizados constantemente para elevar o nível de segurança da informação, levantando métricas sobre a segurança e apontando os principais pontos de atenção.

O Red Team deverá realizar os Pentests, devendo no final de cada Pentest criar o relatório final para enumerar as falhas de segurança encontradas, as quais deverão ser corrigidas pelo Time de Segurança da Informação.

Os Pentests deverão contemplar em seu escopo todos os ambientes em Produção, produtos críticos e ativos presentes no escopo do PCI DSS.

16. POLÍTICA DE FIREWALL

Deverão ser mantidos controles de firewall em todo o ambiente da Superlógica, a fim de prevenir invasões e fortalecer os controles de segurança já implementados em programação.

O Time de Segurança da Informação deverá atualizar a política de firewall de acordo com os incidentes que ocorrerem, para garantir a segurança contra possíveis outras violações.

17. AVALIAÇÃO PERIÓDICA DOS PROCEDIMENTOS

As normas e procedimentos internos deverão ser revisadas periodicamente, devendo ser observada a eficácia e adequação à Política de Segurança da Informação.

A reavaliação deverá ser realizada anualmente e havendo mudanças, essas deverão ser notificadas ao Time de Segurança da Informação para atualizar a presente Política.

18. REVISÃO DA POLÍTICA DE SEGURANÇA

A Política de Segurança da Informação deverá ser revisada anualmente ou sempre que se fizer necessário.

19. SANÇÕES ADMINISTRATIVAS E LEGAIS

O descumprimento ou a inobservância de quaisquer regras ou diretrizes definidas neste instrumento e em suas normas complementares constituem falta grave, sobre as quais a Superlógica aplicará todas as medidas cabíveis nos âmbitos administrativo e judicial, sem prejuízo

de rescisão unilateral e motivada da relação contratual, direta ou indireta, existente entre a parte infratora e a Superlógica.