solo
NETWORK

Política de Segurança da Informação

ABRIL/2024
v.03

1. Sumário

2. Objetivo

O objetivo desta política é estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores da Solo Network adotar padrões de comportamento seguros, adequados às metas e necessidades.
Garantir a confidencialidade, integridade e disponibilidade das informações.
Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, clientes e parceiros.
A Solo Network sempre manterá esta política disponível a todos, atualizada e quando necessário divulgará seu conteúdo e/ou atualizações.

3. Referências

- Norma ABNT NBR ISO/IEC ISO 27001:2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos.
- Norma ABNT NBR ISO/IEC ISO 27701:2019 - Técnicas de segurança.
- Norma ABNT NBR ISO/IEC ISO 37301:2021 - Sistemas de Gestão de Compliance.
- Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018.

4. Abrangência

Esta Política se aplica a todos os colaboradores, ex-colaboradores, prestadores de serviço, ex. prestadores de serviço, qualquer pessoa com poderes de representação da organização e suas controladas direta ou indiretamente respeitando os acordos operacionais estabelecidos, que possuíram, possuem ou virão a possuir acesso às informações da Solo Network e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura.

5. Papéis e responsabilidades

5.1. Todos os colaboradores

- Responsável pelo acesso realizado com a sua identificação e autenticação;

- Deve acessar a informação para desempenhar profissionalmente suas funções relacionadas à Solo Network ou para outras situações formalmente permitidas;
- Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;
- Comunicar a equipe de Segurança da Informação sobre qualquer evento que viole ou possa violar esta Política;
- Assinar o “Termo de aceite da PSI”, formalizando a ciência e o aceite integral das disposições da Política de Segurança da Informação.

5.2. Alta Direção

- Zelar pela manutenção do negócio, dentro de uma perspectiva de longo prazo e de sustentabilidade, que incorpore considerações de ordem econômica, social, ambiental e de boa governança corporativa na definição dos negócios e operações;
- Formular diretrizes para a gestão da Solo Network;
- Apoiar no cumprimento das diretrizes de Segurança da Informação;
- Zelar pela adequação da estrutura de Segurança da Informação.

5.3. Gestores

- Liderar e dirigir ações (incluindo gerenciamento de riscos) e aplicação de recursos para atingir os objetivos da Solo Network;
- Manter um diálogo contínuo com o corpo administrativo e reportar resultados planejados, reais e esperados, vinculados aos objetivos da Solo Network;
- Estabelecer e manter estruturas e processos apropriados para o gerenciamento de operações e riscos (incluindo controle interno);
- Promover os controles necessários às atividades sob responsabilidade de suas áreas, incluindo o monitoramento dos respectivos riscos de Segurança da Informação;
- Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela Solo Network;
- Garantir a observância da Política de Segurança da Informação e sua aplicabilidade para colaboradores e terceiros;
- Tomar as ações cabíveis para se fazer cumprir os termos desta política;
- Propagar a cultura de prevenção a riscos de Segurança da Informação nos times sob sua gestão

5.4. Segurança da Informação

- Implementar e monitorar controles adequados para preservar a Segurança da Informação e o atendimento das políticas e normativos internos da Organização;
- Atuar para prevenir ou responder a riscos e ameaças de Segurança da Informação conforme as normativas estabelecidas;
- Elaborar e manter procedimentos técnicos de Segurança da informação com apoio das áreas da TI e Negócio;
- Propor e administrar projetos e iniciativas relacionadas à Segurança da Informação;
- Estar presente nas áreas de TI e Negócio, atuando de maneira preventiva, sobre os riscos e ameaças de Segurança da Informação;
- Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;
- Prover informações para a tomada de decisões estratégicas relacionadas à Segurança da Informação;
- Manter a estrutura normativa de Segurança da Informação alinhada com as diretrizes da empresa.

5.5. Tecnologia da Informação

- Prover condições que assegurem a adequada identificação, classificação, avaliação, mitigação, gerenciamento e reporte dos riscos de Segurança da Informação e a efetividade dos controles associados considerando também os resultados dos testes de controles;
- Garantir a observância da Política de Segurança da Informação e sua aplicabilidade para colaboradores e terceiros;
- Propagar a cultura de prevenção a riscos de Segurança da Informação nos times sob sua gestão;
- Monitorar e atentar a desvios e rotinas que possam causar a exposição da organização no cenário de Segurança da Informação;
- Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;
- Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela organização.
- Realizar as cópias de segurança do ambiente tecnológico;

- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos nesta política e adicionais;
- Verificar os riscos relativos ao acesso pelos subcontratados, parceiros às instalações da Empresa e seus colaboradores seguirão o procedimento de controle de acesso, para controle e proteção pertinentes dessas instalações.

5.6. Governança, risco, compliance e auditoria

- Prover condições que assegurem a adequada identificação, classificação, avaliação, mitigação, gerenciamento e reporte dos riscos de Segurança da Informação e a efetividade dos controles associados considerando também os resultados dos testes de controles;
- Garantir a conformidade com as expectativas legais, regulatórias e éticas;
- Fornecer expertise complementar, apoio, monitoramento e questionamento quanto ao gerenciamento de riscos, incluindo:
- Desenvolvimento, implantação e melhoria contínua das práticas de gerenciamento de riscos (incluindo controle interno) nos níveis de processo, sistemas e entidades.
- Fornecer análises e reportar sobre a adequação e eficácia do gerenciamento de riscos (incluindo controle interno).
- Manter a prestação de contas primária perante o corpo administrativo e a independência das responsabilidades da gestão;
- Reportar à gestão e ao corpo executivo sobre a adequação e eficácia da governança e do gerenciamento de riscos, para apoiar o atingimento dos objetivos da Solo Network e promover e facilitar a melhoria contínua;
- Reportar ao corpo executivo prejuízos à independência e objetividade e implantar salvaguardas conforme necessário.

5.7. Área Jurídica

- Requerer a inserção de cláusulas que obriguem o cumprimento desta Política de Segurança da Informação e demais leis, regulamentos e normas aplicáveis aos prestadores de serviços, cujos contratos tenham sua análise requerida ao departamento, assegurando que as informações sejam utilizadas apenas para sua finalidade dentro da organização e preservando sua confidencialidade.

5.8. Recursos Humanos

- Disponibilizar a política e as normas de Segurança da Informação para todos os colaboradores e assegurar que estejam cientes das diretrizes, normas e procedimentos internos;
- Garantir que os colaboradores tenham ciência e assinem o Termo de Ciência de Segurança da Informação no processo de integração;
- Notificar o desligamento dos colaboradores a equipe de TI para tomar medidas relativas à segurança da informação, com relação bloqueios, exclusão ou transferência de direitos relativos a sessões/contas;
- Garantir que os ex-colaboradores devolvam todos os ativos de Tecnologia e Segurança da Informação à Empresa.

6. Diretrizes

6.1. Princípios de Segurança

Segurança da Informação pode ser definida como uma série de atividades designadas para garantir a continuidade dos negócios em sistemas de informação, utilizando computadores e redes de computador visando manter a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações garantindo assim um ambiente seguro de sistemas de informação.

Segurança da Informação também significa todas as medidas preventivas, tangíveis e intangíveis, tomadas para que informações sigilosas da empresa, dados pessoais e ativos relativos à segurança da informação não sejam divulgadas a pessoas não autorizadas ou empresas concorrentes, e proteger informações valiosas da Empresa e de clientes de todos os possíveis vazamentos de informações e ameaças diversas.

- **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

6.2. Estrutura

A estrutura de documentos de Segurança da Informação da organização é composta por diretrizes contempladas nas rotinas de Segurança da Informação e outras áreas, as quais são complementares à presente Política. Existem documentos que detalham as diretrizes corporativas a serem cumpridas por todos os colaboradores e terceiros associados à Organização para atingir o objetivo proposto.

- **Arquitetura de Segurança da Informação** - Estabelece e orienta os modelos de referência e componentes tecnológicos de Segurança da Informação a serem utilizados em sistemas de informação, com base em sua criticidade para a Organização.
- **Gestão de ativos tecnológicos** – Estabelece a gestão de ativos físicos e lógicos, considerando além dos ativos internos, também aqueles que podem ser transitados fora do ambiente tecnológico da Organização.
- **Classificação da Informação**: Estabelece as diretrizes para a adequada classificação e proteção da informação de acordo com o nível de confidencialidade e importância que possui para os negócios da Organização.
- **Conscientização em Segurança da Informação** – Elaborar e disseminar o programa de conscientização de Segurança da Informação.
- **Plano de Continuidade de Negócio** – Estabelece e mantém a capacidade de preservação e continuidade dos negócios, considerando o mínimo necessário, ou seja, processos, pessoas, tecnologias e negócios críticos que devem ser mantidos em caso de cenário de crise.
- **Proteção de dados** – Estabelece os padrões de proteção de dados de forma a manter a confidencialidade, integridade e disponibilidade dos dados da Organização.
- **Trabalho remoto** – Estabelece ao colaborador uma modalidade de trabalho para exercer suas atividades profissionais, obedecendo sua jornada de trabalho em sua própria residência, ou em outro ambiente físico fora da empresa.
- **Gestão de Identidades e acessos** – Controla e segrega o acesso a dados e transações, mitigando o excesso de privilégios que possam levar a vazamento de informações, acesso indevido, fraudes ou mesmo ações que impactem a imagem da Organização.
- **Gestão de Riscos** - Estabelece diretrizes adequadas para identificação, avaliação, comunicação, tratamento e aceitação dos riscos que possam definir o nível de aceitação de riscos ocasionar impacto negativo ou positivo.

- **Resposta a incidentes** – Atua sobre incidentes de Segurança da Informação e a resposta a estes visando a redução de impacto provocado por ações indevidas ou em não conformidade com as políticas da Organização.
- **Métricas e relatórios** – Mantém a Organização informada quanto à exposição dos negócios a riscos de Segurança da Informação que possam comprometer a imagem, operações, saúde financeira, compliance ou sua reputação.
- **Segurança de redes** – Mantém a proteção do ambiente de rede da Organização em relação às informações trafegadas, por meio de um conjunto de controles de Segurança da Informação.
- **Operações de Segurança da Informação** – Realiza a sustentação das ferramentas de Segurança da Informação, processos de autorização e atendimento a dúvidas e problemas relacionados à Segurança da Informação.
- **Privacidade** - Preserva a privacidade de dados pessoais, entendidos como aqueles que identificam ou tornam identificáveis pessoas físicas, nos processos de negócio e em canais da Organização, mediante a sua confidencialidade, integridade, finalidade, autenticidade e disponibilidade.
- **Monitoramento de Segurança da Informação** – Monitora, correlaciona, analisa e realiza medições quanto à proteção, desvios de conduta, ações indevidas e/ou não autorizadas, internas e externas, de forma a preservar a segurança dos usuários, clientes, colaboradores, parceiros de negócio e das estratégias da Organização.
- **Segurança de Software** – Preserva a proteção dos sistemas, aplicativos e aplicações web da organização, desde suas etapas de desenvolvimento até a manutenção em ambientes de produção.
- **Estratégia de Segurança da Informação** – Define e dá ciência à Diretoria e áreas influenciadas sobre o alinhamento de Segurança da Informação à estratégia de negócio.
- **Gestão de Segurança da Informação para terceiros** – Estabelece as diretrizes de Segurança da Informação e avalia o cumprimento dos requisitos pelos terceiros no momento da contratação, durante as renovações e o monitoramento contínuo.
- **Inteligência de ameaças** – Mapeia e identifica ameaças de Segurança da Informação que possam comprometer a Organização, possibilitando ações preventivas através de soluções de segurança integradas de tecnologia, processos, procedimentos e pessoas, minimizando possíveis impactos na Organização antes que possam ocorrer, prejudicando a estratégia da organização.
- **Gestão de vulnerabilidades** – Minimiza o risco de Segurança da Informação da Organização mediante a identificação e direcionamento sobre as vulnerabilidades tecnológicas.

- **Segurança em nuvem** – Estabelece as diretrizes de Segurança da Informação e avalia o cumprimento dos requisitos em ambientes e provedores de nuvem, além de realizar o monitoramento contínuo.
- **Segurança física** – Estabelece diretrizes para a proteção física e de perímetro que protege os dados e informações da Organização.
- **Criptografia** – Assegura o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

7. Disposições Gerais

Os casos não previstos neste plano ou as dúvidas porventura existentes, poderão ser tratados pelo interessado junto à Gerência de Segurança da Informação

8. Penalidades

O descumprimento da política pode ocasionar medidas disciplinares

9. Histórico de Revisão

REVISÃO	DATA	DESCRIÇÃO	ELABORADOR	REVISOR	APROVADOR	
					Nome	**Assinatura**
00	26/05/2021	Edição inicial	Luana Santos			
01	08/06/2021	Revisão edição inicial	Carlos Lucas			
02	12/11/2021	Descrição nas tratativas do processo	Luana Santos			
03	08/04/2024	Reestruturação	Sérgio Santos	Felipe Guimarães	Eduardo Martins Felipe Guimarães	Eduardo Martins