POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Última Atualização: Maio de 2022
Classificação da Informação: Uso Público

Definição
Este documento descreve diretrizes sobre a Política de Segurança da Informação da **ROUXINOL,** cujas regras e procedimentos são de cunho confidencial, publicadas internamente. Tais diretrizes orientam o uso aceitável dos ativos de informação da instituição, baseadas nos princípios de confidencialidade, integridade e disponibilidade.

Público Alvo
Funcionários, Terceiros, Prestadores de Serviços, Clientes, Parceiros e Canais de Comunicação.

Objetivo
- Estabelecer diretrizes e normas de Segurança da Informação que permitam aos funcionários da **ROUXINOL TURISMO,** adotar padrões de comportamento seguro, adequadas às suas metas e necessidades;
- Orientar colaboradores quanto a adoção de controles e processos para atendimento dos requisitos de Segurança da Informação;
- Capacitar os funcionários da **ROUXINOL TURISMO,** no que se refere à prevenção, detecção e resposta a incidentes de Segurança da Informação;
- Prevenir possíveis causas de incidentes de Segurança da Informação;
- Resguardar ativos de informação e/ou tecnológicos da **ROUXINOL TURISMO,** garantindo requisitos de confidencialidade, integridade e disponibilidade;
- Minimizar os riscos de perdas financeiras, da confiança do cliente ou de qualquer outro impacto negativo no negócio da **ROUXINOL TURISMO,** como resultado de falhas de segurança.

Responsabilidades
A Política de Segurança da Informação da **ROUXINOL TURISMO,** trata sobre responsabilidades gerais da instituição, de seus colaboradores e terceiros, bem como a Alta Administração.

Conscientização e Treinamentos de Segurança da Informação
A **ROUXINOL,** define diretrizes de educação contínua para o aculturamento de boas práticas de segurança e disseminação para utilização no dia-a-dia dos colaboradores, seja para fins profissionais quanto para fins pessoais. A Política aborda procedimentos utilizados no programa de conscientização da instituição, tais como treinamentos e informativos internos.

Gestão de Riscos de Segurança da Informação
A gestão de riscos cibernéticos é de responsabilidade da área de Segurança da Informação. Este processo identifica os requisitos de segurança relacionado às necessidades da instituição. A gestão de riscos cibernéticos é contínua e define contextos internos e externos para avaliação, além de tratar riscos identificados de modo que sejam reduzidos à níveis aceitáveis.

Gestão de Senhas
A **ROUXINOL TURISMO,** faz o uso das melhores práticas de uso de senhas, exigindo uma complexidade determinada para criação, assim como evita a reutilização de senhas anteriores.
As senhas são geradas com a exigência de caracteres mínimos definidos, bloqueio por tentativa sem sucesso e contém uma periodicidade exigida para alteração.

Gestão dos Ativos
A **ROUXINOL TURISMO,** possui seus ativos de informação identificados, atualizados, classificados, com respectivos proprietários responsabilizados pelo uso aceitável dos ativos, conforme política interna.

Proteção e Classificação da Informação

A **ROUXINOL TURISMO,** estabelece diretrizes para a classificação, manuseio e rotulagem dos ativos de informação da empresa. O documento interno prevê todas as diretrizes utilizadas para a classificação da informação, descreve suas categorias, prevê ainda diretrizes para o manuseio da informação, para o descarte da informação, descreve regras sobre prevenção a vazamento de dados e políticas, sobre cópias e restauração de dados (backup e restore), bem como sobre criptografia.

Uso Aceitável de Recursos Tecnológicos
Os recursos de tecnologia da **ROUXINOL TURISMO,** devem ser utilizados de forma profissional, ética e legal, conforme definido no termo de responsabilidade aplicável. A Política de Segurança da Informação aborda a definição de recursos tecnológicos, além de regras que tratam deste tema, pelas quais os colaboradores e terceiros da **ROUXINOL TURISMO** devem seguir.

Gestão de Identidade e Acessos
A **ROUXINOL TURISMO,** estabelece diretrizes gerais para acesso a ativos e sistemas de informação. Toda gestão de acessos é de responsabilidade da área de Tecnologia da Informação e é baseada no princípio da necessidade de acesso à informação para a execução das atividades laborais do colaborador.
A Política define diretrizes, tais como:

- Perfis de Acessos das Áreas de Negócio;
- Processo de Admissão ou Transferência de Área de Funcionários;
- Processo de Desligamento de Colaboradores;
- Acesso de Terceiros, Visitantes e Temporários;
- Acesso a Banco de Dados;
- Acesso Remoto;
- Acesso Físico;
- Revisão de Acessos;
- Parametrização de Senhas; e
- Múltiplo Fator de Autenticação.

Criptografia
Os ativos de informação da **ROUXINOL TURISMO** possuem criptografia adequada, a fim de garantir a proteção em todo o ciclo de vida da informação, em conformidade com padrões de segurança dos órgãos reguladores.

Desenvolvimento de Software
A **ROUXINOL TURISMO,** desenvolve suas aplicações conforme procedimentos, documentos e instruções de trabalhos internos, seguindo práticas de segurança da informação, alinhado com a Política de Segurança interna.
Os ambientes de produtivos são segregados dos demais ambientes e com acesso por usuários previamente autorizados ou por ferramentas homologadas.
Todos os sistemas ou aplicações adquiridas de terceiros, devem seguir diretrizes definidas na Política de Segurança da Informação e devidamente homologados.

Proteção Contra Códigos Maliciosos
A **ROUXINOL TURISMO,** define diretrizes para a proteção contra ameaças de códigos maliciosos (malwares).

Monitoramento de Segurança
A Política de Segurança da Informação trata sobre o monitoramento de segurança, descrevendo os aspectos necessários para identificação de eventuais ameaças.

Trabalho Remoto
A **ROUXINOL TURISMO,** impõe exigências para trabalho remoto, como o uso de Virtual Private Network (VPN).

Gestão de Vulnerabilidade e Conformidade

A **ROUXINOL TURISMO,** possui processos de gestão de vulnerabilidade e conformidade, de modo que as seguintes diretrizes estão estabelecidas:
• Gestão de Vulnerabilidade;
• Gestão de Conformidade;
• Testes Periódicos de Segurança; e
• Correções de Segurança (Gestão de Patch).

Backup
A **ROUXINOL TURISMO,** adota soluções de Backup e Desaster Recovery para a proteção de seus dados contra perda de informação.
Testes periódicos são adotados para garantir a integridade das informações, averiguar a eficácia dos processos e estabelecer melhorias.

Respostas a Incidentes de Segurança
A **ROUXINOL TURISMO,** define diretrizes para prevenir, responder e tratar adequadamente incidentes de Segurança que estejam impactando ou podem vir a impactar ativos/serviços de informação ou recursos tecnológicos da instituição.
Neste tópico, a Política trata sobre responsabilidades das áreas na prevenção e resposta a incidentes.
Além disso, a Política descreve regras de priorização e severidade com relação a possíveis incidentes, procedimentos sobre a definição de autoridades e regras para a elaboração de cenários de testes de continuidade de negócios.
Cabe ainda ressaltar que a **ROUXINOL TURISMO,** possui um Plano de Respostas a Incidentes, contendo metodologia e diretrizes para o tratamento de incidentes de Segurança Cibernéticas.

Gestão de Continuidade de Negócios
A **ROUXINOL TURISMO,** realiza a gestão de continuidade de negócios com soluções, estratégias e procedimentos a serem executados durante eventuais cenários de contingência alinhados com o propósito e metas estratégicas da instituição. Para tal, a **ROUXINOL TURISMO** possui um Plano de Continuidade de Negócios (PCN) que cumpre funções definidas em documentos internos.

Gestão de Terceiros
A **ROUXINOL TURISMO,** estabelece diretrizes para profissionais terceiros em suas dependências ou para contratação de serviços.
A **ROUXINOL TURISMO,** possui regras de diligência adicionais para terceiros considerados relevantes, que são aqueles que armazenam ou processam dados considerados críticos em estrutura tecnológica não pertencente a **ROUXINOL TURISMO.**

Segurança em Dispositivos Móveis
A **ROUXINOL,** define diretrizes para utilização segura de dispositivos móveis, bem como as atribuições das áreas responsáveis pelo monitoramento.

Segurança em Redes
A **ROUXINOL TURISMO,** possui ferramentas de segurança capazes de detectar e responder tentativas de intrusão e seu ambiente. No presenta tópico, a Política aborda, também, regras sobre a rede Sem Fio corporativa e pública.

Privacidade de Dados Pessoais
A **ROUXINOL,** garante que o propósito do tratamento dos dados pessoais são sejam ilícitos ou abusivos, assim como garante o direito fundamentais à privacidade relativas a LGPD – Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018).

Sanções e Punições
A área de Segurança da Informação realiza o monitoramento contínuo do ambiente tecnológico por meio de métodos diversos para assegurar a conformidade e adesão a esta Política. Caso haja violação das regras nela dispostas, bem como as demais normas e procedimentos de Segurança da Informação, mesmo que

por omissão ou tentativa não consumada, tal violação pode ser classificada como incidente de Segurança da Informação, os quais são passíveis de penalidades.
As demais sanções e punições para o descumprimento das regras de Segurança da Informação estão descritas na Política interna.

* * *