Política de Segurança da Informação

- Versão: 1.0.
- Data de Publicação: 27/10/2024.
- Departamento: Tecnologia da Informação / Segurança da Informação.

1. Introdução

1.1. Objetivo

Esta política tem como principal objetivo estabelecer diretrizes que assegurem a proteção e a gestão de informações e ativos digitais da Sabor do Campo. Ao estabelecer um conjunto abrangente de requisitos e práticas, a empresa visa criar um ambiente seguro e confiável para todos os seus dados, sistemas e operações, alinhando-se a normas e padrões de segurança da informação.

1.2. Escopo

Aplicável a todos os funcionários, prestadores de serviço, fornecedores e parceiros da Sabor do Campo, esta política cobre todos os níveis de interação com informações e sistemas da empresa. O escopo inclui desde o uso adequado de dados pessoais e corporativos até a proteção dos sistemas e ativos digitais essenciais, abrangendo as exigências de conformidade e proteção de dados.

2. Diretrizes Fundamentais de Segurança

2.1. Confidencialidade

A Sabor do Campo adota práticas rigorosas para garantir que informações sensíveis e confidenciais sejam acessíveis exclusivamente a pessoas autorizadas. Medidas de proteção como criptografia de dados, segregação de funções e monitoramento de acessos são adotadas para prevenir a exposição e garantir que os dados permaneçam seguros em todo o ciclo de vida da informação.

2.2. Integridade

A integridade das informações é mantida por meio de controles de qualidade que impedem alterações não autorizadas ou acidentais, protegendo a precisão e consistência dos dados. A Sabor do Campo realiza auditorias regulares e conta com sistemas de detecção de fraudes para assegurar que as informações de negócios, financeiros e de clientes se mantenham íntegras e confiáveis.

2.3. Disponibilidade

Para que os dados e sistemas da empresa estejam sempre acessíveis, a Sabor do Campo adota políticas de backup, redundância e recuperação de desastres. A infraestrutura de TI é projetada para assegurar a continuidade dos serviços e minimizar o impacto de falhas, permitindo uma rápida recuperação em caso de incidentes e garantindo que as operações não sejam comprometidas.

3. Gerenciamento e Controle de Acesso

3.1. Controle de Acesso Baseado em Funções (RBAC)

O acesso aos dados e sistemas é controlado com base nas funções e responsabilidades de cada colaborador. A Sabor do Campo utiliza o Controle de Acesso Baseado em Funções (RBAC), atribuindo níveis específicos de permissão para que cada usuário possa acessar apenas as informações necessárias. Esse sistema é revisado periodicamente e atualizado conforme alterações nas funções ou desligamento de colaboradores.

3.2. Mecanismos Avançados de Autenticação

Os sistemas da empresa são protegidos por autenticação multifatorial (MFA), adicionando uma camada extra de segurança aos acessos. A combinação de fatores, como senhas, tokens e biometria, minimiza o risco de acessos indevidos e reforça a segurança das informações e processos.

3.3. Autorização e Regras de Uso

As permissões de acesso são concedidas conforme a necessidade de trabalho, garantindo que cada colaborador acesse apenas o que é essencial para sua função. A Sabor do Campo monitora continuamente os acessos e realiza auditorias para identificar e corrigir eventuais abusos ou desvios, mantendo a conformidade e segurança dos dados.

4. Segurança Física e Proteção Ambiental

4.1. Proteção da Infraestrutura

As instalações da Sabor do Campo são protegidas contra acessos físicos não autorizados por meio de câmeras de vigilância, controles de acesso e segurança em tempo integral. As áreas que armazenam informações sensíveis ou equipamentos de TI são monitoradas e restritas a pessoal autorizado, assegurando que a infraestrutura crítica esteja resguardada.

4.2. Controles de Acesso Físico Personalizados

Locais de acesso restrito, como os centros de dados e servidores, contam com sistemas de controle de acesso físico, incluindo cartões de identificação e biometria. Somente funcionários previamente autorizados podem acessar essas áreas, e todas as entradas e saídas são registradas para fins de auditoria e controle.

4.3. Mitigação de Riscos Ambientais

A empresa adota práticas de mitigação de riscos ambientais, como sistemas de controle de temperatura, umidade, sensores de fumaça e procedimentos de emergência. Esses controles garantem a proteção dos dados e a continuidade das operações mesmo em situações adversas, como incêndios ou enchentes.

5. Segurança de Redes e Comunicações

5.1. Segurança de Perímetro e Segurança Interna de Redes

A Sabor do Campo utiliza firewalls e sistemas de prevenção de intrusão para proteger sua rede contra ameaças externas e internas. A segmentação da rede é implementada para que diferentes áreas da empresa tenham acesso controlado, minimizando o risco de um ataque afetar toda a infraestrutura.

5.2. Monitoramento Contínuo e Análise de Tráfego

As redes da empresa são monitoradas 24/7 para detectar e bloquear acessos não autorizados. Utilizamos soluções de segurança avançadas para identificar padrões incomuns e responder a ameaças em tempo real, garantindo que o ambiente digital permaneça seguro e protegido contra intrusões.

6. Gerenciamento e Resposta a Incidentes de Segurança

6.1. Estrutura de Resposta a Incidentes

A equipe de segurança da Sabor do Campo segue um plano estruturado de resposta a incidentes, que cobre desde a identificação de ameaças até a recuperação completa dos sistemas. Esse processo inclui análise detalhada do incidente, resposta rápida para minimizar danos e medidas preventivas para evitar recorrências.

6.2. Notificação e Relatório de Incidentes

Todos os incidentes de segurança são documentados e relatados para análise interna e melhoria contínua. A equipe responsável informa a liderança e elabora relatórios que descrevem o incidente, suas causas, medidas tomadas e sugestões para aperfeiçoar a segurança da informação.

7. Conscientização e Treinamento em Segurança

7.1. Programa de Sensibilização para Boas Práticas

A Sabor do Campo promove uma cultura de segurança através de campanhas educativas e treinamentos regulares para conscientizar os colaboradores sobre os riscos e as melhores práticas de segurança da informação. Mensagens de conscientização são divulgadas periodicamente para reforçar o comprometimento de todos com a proteção dos dados.

7.2. Capacitação Técnica e Treinamento Periódico

Os colaboradores recebem treinamentos adaptados às suas funções para assegurar que compreendam as responsabilidades em relação à segurança da informação. Esses treinamentos são atualizados periodicamente e incluem práticas de prevenção contra phishing, gestão de senhas e segurança digital.

8. Avaliação e Melhoria Contínua

8.1. Auditorias de segurança

Auditorias internas e externas são conduzidas para avaliar a conformidade com as políticas de segurança e identificar oportunidades de melhoria. As inspeções garantem que a Sabor do Campo mantenha altos padrões de segurança e que os controles implementados estejam funcionando conforme planejado.

8.2. Revisão de políticas e procedimentos

Nossos protocolos e procedimentos de segurança são revisados semestralmente ou sempre que houver uma atualização significativa no ambiente de TI ou nas ameaças. Essas revisões garantem que a Sabor do Campo esteja sempre alinhada com as melhores práticas e pronta para responder a novos desafios.

8.3. Análise de riscos

A empresa realiza análises de risco periódicas para identificar vulnerabilidades e implementar medidas de mitigação proativas. Esse processo permite uma visão completa das possíveis ameaças e oferece uma base sólida para o planejamento de ações preventivas e corretivas.

8.4. Medição de desempenho

Indicadores de desempenho, como tempo de resposta a incidentes e número de tentativas de acesso bloqueadas, são monitorados para avaliar a eficácia das políticas de segurança. Esses KPIs “Key Performance Indicators” (Indicadores-Chave de Desempenho) ajudam a Sabor do Campo a ajustar suas práticas e a atingir os objetivos de segurança definidos.

9. Conformidade Legal e Regulatória

9.1. Conformidade com leis e regulamentações

A Sabor do Campo adere rigorosamente a todas as leis e regulamentações aplicáveis, incluindo a LGPD e normas internacionais, garantindo que as práticas de segurança atendam a todas as exigências de privacidade e proteção de dados.

9.2. Gerenciamento de vulnerabilidades e patches

A empresa segue um processo estruturado para identificar, avaliar e corrigir vulnerabilidades em seus sistemas e aplicativos. Atualizações de segurança (patches) são aplicadas regularmente para assegurar que todos os sistemas estejam protegidos contra vulnerabilidades conhecidas.

10. Política de Proibição de Dispositivos Pessoais para Atividades Corporativas

10.1. Objetivo

Estabelecer uma diretriz que proíba o uso de dispositivos pessoais (como notebooks, smartphones e tablets) para quaisquer atividades relacionadas ao trabalho dentro da organização, com o objetivo de proteger a segurança da informação, a privacidade dos dados e manter o controle completo sobre os ativos de TI.

10.2. Diretrizes

Proibição de BYOD (Bring Your Own Device):
Em virtude dos riscos associados ao uso de dispositivos pessoais no ambiente de trabalho, como falta de controle de segurança, exposição a malwares e dificuldades em aplicar políticas de segurança, fica proibida a prática de BYOD. Colaboradores não devem utilizar dispositivos próprios para realizar tarefas ou acessar informações relacionadas ao trabalho.

Acesso Exclusivo por Dispositivos Corporativos:
Todo acesso aos sistemas e dados da empresa deve ser realizado exclusivamente por dispositivos fornecidos pela Sabor do Campo. Esses dispositivos são configurados e mantidos pela equipe de TI para garantir a conformidade com os padrões de segurança da informação e proteger os dados corporativos.

Segurança e Monitoramento:
A equipe de TI da empresa é responsável pela configuração, manutenção e monitoramento dos dispositivos

corporativos, garantindo que estejam protegidos contra ameaças cibernéticas. O uso de dispositivos pessoais compromete essa proteção e representa um risco direto à segurança da empresa.

Exceções e Autorização Prévia:
Qualquer exceção a esta política deve ser aprovada por escrito pela diretoria de TI e apenas em circunstâncias específicas e justificadas. Tais exceções estão sujeitas a revisões periódicas e podem ser revogadas a qualquer momento se comprometerem a segurança da organização.

10.3. Penalidades

O não cumprimento desta política pode resultar em medidas disciplinares, incluindo advertências e sanções que vão de acordo com a gravidade da violação, conforme previsto nas normas internas da empresa e nas leis trabalhistas aplicáveis.

10.4. Justificativa

Essa política visa mitigar os riscos associados ao uso de dispositivos pessoais, como perda de dados, brechas de segurança, distração digital e comprometimento da privacidade dos dados corporativos e pessoais, alinhando-se às melhores práticas de segurança da informação.

11. Papéis e Responsabilidades

11.1. Direção

A direção é responsável por apoiar e supervisionar as iniciativas de segurança, assegurando que os recursos necessários estejam disponíveis para a implementação eficaz das políticas de segurança e promovendo uma cultura de segurança em toda a organização.

11.2. Equipe de Segurança da Informação

A equipe de segurança da informação é encarregada de planejar, monitorar e executar os protocolos de segurança, além de responder a incidentes e garantir que as políticas sejam cumpridas. A equipe também realiza treinamentos e auditorias para manter os padrões de segurança elevados.

11.3. Compromisso dos Colaboradores

Todos os colaboradores têm o compromisso de seguir as políticas de segurança estabelecidas e de relatar quaisquer incidentes ou irregularidades que possam comprometer a segurança da empresa. A colaboração de todos é fundamental para garantir a proteção dos dados e a segurança organizacional.

12. Conclusão

12.1. Encerramento

Todos os colaboradores têm o compromisso de seguir as políticas de segurança estabelecidas e de relatar quaisquer incidentes ou irregularidades que possam comprometer a segurança da empresa. A colaboração de todos é fundamental para garantir a proteção dos dados e a segurança organizacional.