POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

CLASSIFICAÇÃO: PÚBLICO

Sumário

1.Introdução

A AIQON entende que é essencial para a proteção dos ativos, reputação e continuidade das operações, estabelecer diretrizes para o gerenciamento da segurança da informação em conformidade com a norma ABNT NBR ISO/IEC27001 DE 11/2022 e os controles especificados no Anexo A da norma ABNT NBR ISO/IEC27001 DE 11/2022.

2.Controle de Versões

Versão	Data	Descrição	Autor
1.0	29/05/2023	Emissão do Documento	Edson Oguma
2.0	07/12/2023	Revisão do Documento	Edson Oguma
3.0	29/09/2024	Revisão e atualização dos itens da política	Edson Oguma
4.0	01/04/2025	Revisão do Documento	Edson Oguma, Gizelle Silva

Esta política é revisada e/ou atualizada anualmente ou quando houver necessidade do negócio.

Elaborado por: Edson Oguma	Aprovado por: Matheus Nascimento

3.Escopo

Esta política se aplica a todas as áreas da organização.

4.Termos e Definições

Confidencialidade: Garantir que a informação está acessível somente a indivíduos autorizados, prevenindo o acesso não autorizado.

Integridade: A propriedade de manter a exatidão e a completude da informação, prevenindo alterações não autorizadas.

Disponibilidade: A garantia de que os sistemas de informação e os dados estão acessíveis e utilizáveis quando necessário por pessoas autorizadas.

Sistema de Gestão de Segurança da Informação (SGSI): Conjunto de políticas, procedimentos e controles implementados para gerenciar a segurança da informação e garantir conformidade com a ABNT NBR ISO/IEC27001 DE 11/2022.

Incidente de Segurança: Evento que possa resultar em uma falha na confidencialidade, integridade ou disponibilidade das informações. Podendo ser um ataque cibernético, violação de políticas, vazamento de dados etc.

5.Responsabilidades

Alta Direção:

Demonstrar compromisso com a segurança da informação e com o cumprimento da política.

Apoiar iniciativas, projetos e investimentos em segurança da informação.

Elaborado por: Edson Oguma	Aprovado por: Matheus Nascimento

Garantir que a política seja implementada, revisada e comunicada a toda a organização.

Promover uma cultura de segurança entre líderes e colaboradores.

Disponibilizar recursos necessários para a implementação e manutenção do SGSI.

ITSEC:

Proteger redes, sistemas e dados contra acessos não autorizados.

Assegurar a aplicação de atualizações, backups e mecanismos de controle de acesso.

Monitorar e registrar atividades nos ambientes de TI.

Apoiar a implementação de soluções seguras de hardware e software.

Definir, implementar e manter controles de segurança adequados.

Monitorar riscos, ameaças e vulnerabilidades.

Investigar incidentes de segurança e propor ações corretivas e preventivas.

Gestores de Áreas:

Assegurar que os colaboradores sob sua responsabilidade cumpram a política.

Validar os acessos a sistemas e dados da sua equipe.

Reportar incidentes ou não conformidades de segurança à área responsável.

Responsável por Compliance:

Avaliar a conformidade com políticas, normas e legislações.

Promover treinamentos de conscientização sobre segurança da informação.

Elaborado por: Edson Oguma	Aprovado por: Matheus Nascimento

Realizar auditorias e acompanhar planos de ação relacionados à segurança.

Atualizar e revisar políticas, procedimentos e normas relacionados à segurança

Colaboradores:

Proteger senhas, equipamentos e informações sob sua responsabilidade.

Cumprir as diretrizes da política e dos treinamentos de segurança.

Reportar comportamentos suspeitos, falhas ou incidentes imediatamente.

Não compartilhar credenciais nem instalar softwares não autorizados.

Participar de treinamentos e programas de conscientização em segurança da informação.

Partes Interessadas:

Cumprir os termos contratuais relacionados à segurança da informação, incluindo cláusulas de confidencialidade, proteção de dados e afins.

Adotar práticas de segurança compatíveis com as exigências da organização, principalmente quando houver acesso a informações, sistemas ou infraestrutura.

Comunicar imediatamente qualquer incidente, falha ou suspeita de violação de segurança ao ponto de contato designado.

Participar, quando exigido, de treinamentos, avaliações ou homologações de segurança.

Respeitar os níveis de acesso concedidos, sem tentar obter informações além do necessário para a execução dos serviços.

6. Princípios Fundamentais da Segurança da Informação

Confidencialidade

Garantir que apenas pessoas autorizadas tenham acesso à informação.

- Objetivo: Evitar o acesso não autorizado.
- Exemplos de aplicação:
    - Controle de acesso (usuário e senha, autenticação multifator).
    - Criptografia de dados.
    - Políticas de sigilo e confidencialidade.

Integridade

Assegurar que a informação não seja alterada indevidamente, durante o armazenamento ou transmissão.

- Objetivo: Garantir que os dados estejam corretos e completos.
- Exemplos de aplicação:
    - Assinaturas digitais.
    - Checksums e hash (verificação de integridade).
    - Controle de versões e logs de alterações.

Disponibilidade

Garantir que a informação esteja acessível sempre que necessário, para pessoas autorizadas.

- Objetivo: Manter os serviços e dados disponíveis em tempo hábil.
- Exemplos de aplicação:

- Backup e recuperação de desastres.
- Redundância de sistemas.
- Monitoramento e manutenção contínua.

7.Diretrizes

7.1 Recursos

A organização deve assegurar a disponibilização de recursos adequados para garantir a implementação e manutenção das medidas de segurança da informação, incluindo:

Investimento contínuo em tecnologia e infraestrutura de segurança;

Disponibilidade de equipe qualificada para suporte às atividades de segurança;

Alocação de orçamento para treinamentos, auditorias e certificações.

7.2 Competência

A organização deve assegurar que todos os colaboradores possuam as competências necessárias para desempenhar suas funções em segurança da informação, por meio de:

Definição de requisitos mínimos de competência para cada função relacionada à segurança;

Programas de capacitação contínua para atualização de conhecimentos técnicos;

Avaliação periódica de desempenho e competências para ajustes necessários.

7.3 Conscientização

Para reforçar a cultura de segurança da informação, serão implementadas iniciativas de conscientização, incluindo:

Campanhas regulares sobre boas práticas de segurança da informação;

Treinamentos para todos os colaboradores e partes interessadas com acesso a informações sensíveis;

Comunicação de alertas de segurança e lições aprendidas sobre incidentes.

7.4 Comunicação

A comunicação sobre segurança da informação será estruturada e acessível a todos os colaboradores, considerando:

Canais formais utilizado pela organização para disseminação de políticas e diretrizes de segurança;

Disponibilização de relatórios de segurança para a alta administração e reuniões para tratar sobre o assunto;

Criação de um canal para reportar de forma segura e confidencial de incidentes de segurança.

7.5 Informação Documentada

A organização manterá informações documentadas para garantir a efetividade e rastreabilidade das políticas e processos de segurança da informação, incluindo:

Registro formal de políticas, procedimentos e normas internas de segurança;

Estrutura básica com título, controle de versões, classificação, elaborador e aprovador mantendo o controle de acesso aos documentos relevantes;

Revisão periódica das informações documentadas para alinhamento com requisitos regulatórios e melhores práticas.

7.6 Gestão de Riscos

A organização deve implementar uma metodologia formal de gestão de riscos, incluindo:

Identificação e avaliação das vulnerabilidades, ameaças e impactos associados;

Determinação e aplicação de controles adequados para mitigar riscos identificados;

Revisão periódica dos riscos para garantir que as ações corretivas sejam eficazes.

7.7 Segurança de Recursos Humanos

A organização deve adotar práticas de segurança para colaboradores e terceiros, que incluam:

Análise de Due Diligence para novos funcionários com acesso a informações sensíveis e confidencias;

Treinamento contínuo em segurança da informação para todos os colaboradores;

Revogação imediata de acessos e devolução de credenciais ao término do vínculo empregatício.

7.8 Classificação e Controle de Ativos

A organização deve estabelecer um controle rigoroso sobre ativos de informação, que incluam:

Inventário atualizado de ativos;

Classificação da informação em níveis de sensibilidade: Pública, Interna e Confidencial;

Definição de medidas de proteção adequadas conforme a classificação da informação.

7.9 Controles de Acesso

A organização deve conceder acessos com base na necessidade, contendo:

Aplicação do princípio do menor privilégio para todos os usuários;

Implementação de autenticação multifator para sistemas críticos;

Revisão periódica de acessos e senhas conforme a política vigente.

7.10 Segurança Física e do Ambiente

A organização deve adotar medidas para proteger suas instalações, incluindo:

Controle de acesso físico, vigilância por vídeo e barreiras físicas;

Proteção dos equipamentos contra roubo, danos físicos e desastres naturais;

Restrições de acesso a áreas críticas, como salas de servidores.

7.11 Gestão Operacional da Segurança

A organização deve estabelecer processos operacionais visando a segurança da informação, incluindo:

Documentação e revisão periódica de procedimentos operacionais;

Utilização de soluções atualizadas de proteção contra malware;

Realização de backups regulares e testes de recuperação de desastres;

Monitoramento contínuo de logs de auditoria para detecção de incidentes.

7.12 Manutenção de Sistemas

A organização deve realizar manutenção proativa de seus sistemas, incluindo:

Atualização periódica de softwares e aplicações críticas;

Condução de testes regulares de segurança, como análise de vulnerabilidades e testes de penetração.

7.13 Relacionamento com Fornecedores

A organização deve estabelecer controles sobre terceiros com acesso a informações, incluindo:

Avaliação de riscos e exigência de contratos com cláusulas de segurança da informação e proteção de dados;

Monitoramento contínuo do cumprimento dos requisitos de segurança da informação para os fornecedores.

7.14 Gestão de Incidentes de Segurança

A organização deve ter um processo formal de resposta a incidentes, incluindo:

Registro e investigação dos incidentes de segurança;

Procedimentos definidos para contenção, mitigação e recuperação de eventos;

Treinamento de colaboradores para relatar qualquer anomalia ou incidente.

7.15 Continuidade de Negócios

A organização deve implementar estratégias para assegurar a continuidade dos negócios em caso de incidentes de segurança da informação, incluindo:

Um Plano de Continuidade de Negócios (PCN) testado periodicamente;

Um Plano de Recuperação de Desastres (PRD) para rápida restauração de sistemas.

7.16 Conformidade

A organização deve assegurar o cumprimento de normas e regulamentos aplicáveis, incluindo:

Monitoramento e conformidade com requisitos legais e regulatórios.

Realização de auditorias internas e externas.

7.17 Melhoria Contínua

A organização deve promover revisões regulares no SGSI, incluindo:

Identificação de oportunidades de melhoria com base em novas ameaças e tecnologias;

Adaptação contínua dos controles de segurança da informação para melhor proteção da organização.

8.Sanções

A violação desta política pode resultar em ações disciplinares e consequências legais.

9.Referências

ABNT NBR ISO/IEC27001 DE 11/2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação – Requisitos

ABNT NBR ISO/IEC27002 DE 10/2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação.

Anexo 1 - De Responsabilidade

Eu, _____ na presente data _____, declaro que estou ciente sobre o documento da política de segurança da informação da AIQON, assim como assumo o compromisso de cumpri-las integralmente.

_____

Assinatura

Elaborado por: Edson Oguma	Aprovado por: Matheus Nascimento