POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SISTEMA DE GESTÃO INTEGRADO

ISO 27001

1 – INTRODUÇÃO

A AIQON entende que a segurança da informação é essencial para a proteção dos ativos, reputação e continuidade das operações da organização. Esta política estabelece as diretrizes para o gerenciamento da segurança da informação em conformidade com a norma ISO/IEC 27001:2022 e os controles especificados no Anexo A da norma ISO/IEC 27001.

2 – OBJETIVO

O objetivo desta política é garantir a proteção da informação contra ameaças, garantir a confidencialidade, integridade e disponibilidade das informações e assegurar que a empresa esteja em conformidade com os requisitos da ISO/IEC 27001.

3 – ESCOPO

Esta política abrange todos os ativos de informação, processos e sistemas que são geridos ou operados pela AIQON, bem como todos os colaboradores, prestadores de serviços, fornecedores e parceiros que têm acesso a esses ativos.

4 – TERMOS E DEFINIÇÕES

Ativos de Informação: Se a organização já entende o que são ativos de informação, esse termo pode ser omitido.
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 ISO/IEC 27001.
Incidente de Segurança: Evento que pode resultar em uma falha na confidencialidade, integridade ou disponibilidade das informações. Pode ser um ataque cibernético, violação de políticas, vazamento de dados, etc.
Vulnerabilidade: Fraqueza em um sistema, processo ou controle que pode ser explorada por uma ameaça para comprometer a segurança da informação.

5 – DECLARAÇÃO DE APLICABILIDADE

A Declaração de Aplicabilidade define os controles de segurança que serão implementados de acordo com norma ISO/IEC 27001. O documento complementa a política e é uma parte essencial do SGSI.

6 – PRINCÍPIOS FUNDAMENTAIS DA SEGURANÇA DA INFORMAÇÃO

6.1 Confidencialidade

A informação deve ser acessível apenas a indivíduos autorizados.

6.2 Integridade

A precisão e integridade dos dados devem ser protegidas contra modificação não autorizada.

6.3 Disponibilidade

Os sistemas de informação e dados devem estar disponíveis sempre que necessário para os usuários autorizados.

7 – RESPONSABILIDADES E PAPÉIS NA SEGURANÇA DA INFORMAÇÃO

7.1 Alta Direção:

Aprovar e endossar a política de segurança da informação.
Garantir que a segurança da informação esteja alinhada com os objetivos estratégicos da organização.
Disponibilizar recursos necessários para a implementação e manutenção do SGSI.
Realizar revisões periódicas do SGSI e da política de segurança da informação.

7.2 Gestor de Segurança da Informação (GSI)

O GSI é responsável por gerenciar o SGSI, desenvolver políticas, realizar avaliações de riscos e garantir que os controles de segurança estejam em vigor e funcionando.

7.3 Auditores Internos:

Conduzir auditorias internas do SGSI para garantir conformidade com a ISO 27001.
Identificar não conformidades e recomendar ações corretivas.
Reportar os resultados das auditorias à alta direção e ao comitê de segurança da informação.

7.4 Departamento de compliance:

Monitorar e garantir a conformidade com esta política.

7.5 Colaboradores:

Cumprir a política de segurança da informação e os procedimentos relacionados.
Proteger informações confidenciais e sensíveis.
Reportar imediatamente quaisquer incidentes ou suspeitas de incidentes de segurança.
Participar em treinamentos e programas de conscientização em segurança da informação.

7.6 Parte externa: É responsável por seguir as diretrizes contidas a essa política quando houver relação com a AIQON.

7.7 Auditores Internos:
Conduzir auditorias internas do SGSI para garantir conformidade com a ISO 27001.
Identificar não conformidades e recomendar ações corretivas.
Reportar os resultados das auditorias à alta direção e ao comitê de segurança da informação

8 – DIRETRIZES

1. Gestão de Riscos
1.1 Metodologia de Avaliação de Riscos
A organização implementará uma metodologia formal de gestão de riscos, que incluirá:

Identificação das vulnerabilidades.
Avaliação das ameaças e impactos associados.
Determinação de controles adequados para tratar os riscos identificados.

7.2 Tratamento de Riscos
Os riscos identificados serão tratados através de mitigação, aceitação, transferência, com base na análise de risco.

2. Segurança de Recursos Humanos
2.1 Antes da Contratação
Verificações devem ser realizadas para todos os novos funcionários que tenham acesso a informações sensíveis.

2.2 Durante a Contratação
Todos os colaboradores devem ser submetidos a treinamentos regulares de conscientização sobre segurança da informação.

2.3 Após o Término da Contratação
Ao término da relação de trabalho, os acessos aos sistemas devem ser revogados imediatamente, e todas as credenciais e dispositivos devem ser devolvidos.

3. Classificação e Controle de Ativos
3.1 Inventário de Ativos

Todos os ativos de informação devem ser documentados em um inventário de ativos que identifique o proprietário, classificação e uso de cada ativo.

3.2 Classificação da Informação

As informações devem ser classificadas de acordo com o nível de sensibilidade:

Pública: Pode ser divulgada sem restrições.
Interno: Só podem ser divulgadas entre os colaboradores da organização.
Confidencial: Requer medidas de proteção moderadas.

4. Controles de Acesso

4.1 Princípio do Menor Privilégio

O acesso aos sistemas e informações será concedido apenas com base na necessidade, de acordo com as funções de cada colaborador.

4.2 Autenticação e Autorização

Sistemas críticos requerem autenticação multifator (MFA) para proteger contra acessos não autorizados.

4.3 Política de Senhas

Senhas devem ser fortes e alteradas regularmente, seguindo diretrizes estipuladas no documento: POL_2023_2.0_PGS_Política de Gestão de Senhas.

4.4 Gestão de Identidades

Todos os acessos e identidades de usuários devem ser monitorados e revisados regularmente para assegurar conformidade com o documento: POL_2023_2.0_PCA_Política de Controle de Acesso.

5. Segurança Física e do Ambiente

5.1 Proteção das Instalações

As instalações devem ter controles de acesso físico, como cartões de entrada, vigilância por vídeo e barreiras físicas, mas não só se limitando a esses exemplos.

5.2 Proteção de Equipamentos

Todos os equipamentos de TI devem ser protegidos contra roubo, danos físicos e interferências. Deve haver uma proteção robusta contra incêndios e desastres naturais.

5.3 Áreas Seguras

Áreas críticas, como salas de servidores, devem ter controles de acesso restrito.

6. Gestão Operacional da Segurança

6.1 Documentação dos Procedimentos Operacionais

Todos os procedimentos relacionados à segurança da informação devem ser documentados e revisados periodicamente.

6.2 Proteção contra Malware

A empresa deve manter sistemas atualizados de proteção contra malware, com verificação contínua de vírus e vulnerabilidades.

6.3 Backups e Recuperação de Desastres

Devem ser realizadas cópias de segurança regulares, e os planos de backup e recuperação devem ser testados periodicamente.

6.4 Monitoramento e Logs

A empresa manterá logs de auditoria de todos os sistemas críticos para detectar e responder a possíveis violações de segurança.

7. Manutenção de Sistemas

7.2 Testes de Segurança

Todos os sistemas críticos serão submetidos a testes de segurança regulares, como análise de vulnerabilidades e testes de penetração.

8. Relacionamento com Fornecedores

8.1 Gestão de Riscos de Terceiros

Todos os fornecedores que têm acesso às informações da organização devem passar por uma análise, e devem assinar acordos de confidencialidade e contratos de segurança.

8.2 Monitoramento de Contratos

Os contratos devem ser monitorados para garantir que as cláusulas de segurança estão sendo cumpridas.

9. Gestão de Incidentes de Segurança da Informação

9.1 Relato de Incidentes

Todos os incidentes de segurança devem ser registrados e investigados. Colaboradores são responsáveis por relatar qualquer anomalia ou incidente imediatamente.

9.2 Resposta a Incidentes

A organização deve ter um plano formal de resposta a incidentes, que inclua procedimentos para contenção, mitigação e recuperação de eventos de segurança.

10. Continuidade de Negócios

10.1 Plano de Continuidade de Negócios (PCN)

Um Plano de Continuidade de Negócios deve ser mantido para assegurar que as operações essenciais possam continuar durante uma interrupção.

11.2 Plano de Recuperação de Desastres (PRD)

O Plano de Recuperação de Desastres deve garantir a restauração rápida e eficaz de sistemas críticos.

12. Conformidade

12.1 Cumprimento de Requisitos Legais e Regulamentares

A organização deve assegurar que todos os requisitos legais e regulatórios são cumpridos.

12.2 Auditorias Internas e Externas

A organização deve realizar auditorias internas regulares e estar preparada para auditorias externas como parte do processo de certificação ISO 27001.

13. Melhoria Contínua

O SGSI será revisado regularmente para identificar áreas de melhoria e adaptar-se a novas ameaças, tecnologias ou mudanças no ambiente de negócios.

7 – CONFORMIDADE E APLICAÇÃO

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

8 – REVISÃO E ATUALIZAÇÃO

Esta política deve ser revisada e/ou atualizada anualmente ou quando houver necessidade para garantir que continue sendo eficaz e relevante para as necessidades de negócios.

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

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.
ABNT NBR ISO/IEC27701 DE 11/2019 - Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.
ABNT NBR ISO/IEC 31000:2018 – Gestão de riscos — Diretrizes.
ABNT NBR ISO/IEC27701 DE 05/2023 - Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação.
POL_2023_2.0_PGR_Política de Gestão de Riscos
POL_2023_2.0_PRH_Política de Recursos Humanos
POL_2023_2.0_PGA_Política de Gestão de Ativos
POL_2023_2.0_PUA_Politica de Uso Aceitável de Ativos
POL_2023_2.0_PCA_Política de Controle de Acesso
POL_2023_2.0_PGS_Política de Gestão de Senhas
POL_2023_2.0_PSFA_Política de Segurança Física e Ambiente
POL_2023_2.0_PDMW_Política de Defesa de Malware
POL_2024_2.0_PBR_Política de Backup e Restauração
POL_2023_2.0_PRCS-Política de Relacionamento na Cadeia de Suprimento
POL_2023_2.0_PGI_Política de Gestão de Incidentes
POL_2023_2.0_PCN_Política de Continuidade de Negócio

10 – DATA DE VIGÊNCIA

Este documento é válido a partir da data de aprovação.

11 – Comprovação da ciência da presente política

Eu, _____ na presente data _____, declaro que estou ciente sobre o documento de Política de Segurança da Infromação da AIQON, assim como assumo o compromisso de cumpri-las perante a AIQON.

_____

Assinatura