POLÍTICA DE SEGURANÇA CIBERNÉTICA

PO.SEGINFO.0002

PÚBLICO

Este documento é aplicável às empresas do Grupo Acqio.

Publicado em: 02/2024 Versão: 01/2024 Revisão até: 02/2025.

ELABORAÇÃO

Cesar Searlini

CTO

APROVAÇÃO

Gustavo Danzi de Andrade

CEO

ÍNDICE

1. OBJETIVO

A Política de Segurança da Informação e Cibernética ("Política") da Acqio estabelece de maneira formal as diretrizes adotadas pela empresa para disciplinar os procedimentos necessários à proteção de informações e dados, através de regras relacionadas à segurança, cujo principal objetivo é minimizar os riscos relativos a aos ativos da Acqio, garantindo assim, os princípios da confidencialidade, integridade e disponibilidade das Informações da Acqio, seus parceiros, clientes e todos os participantes de seu ecossistema.

2. SIGLAS E TERMOS

- Grupo Acqio: Todas as empresas da Acqio, incluindo Acqio Instituição de Pagamento SA, Esfera 5 ltda, Acqio Holding Participações, Acqio Franchising, Acqio Pagamentos, e Acqio Holding Financeira.
- Ativo: No contexto de Segurança da Informação, é qualquer elemento que gera valor ao negócio, podendo ser informações, pessoas, equipamentos ou sistemas.
- Autenticidade: Propriedade pela qual se assegura que a informação foi produzida ou expedida, modificada ou destruída por uma pessoa natural, equipamento, sistema, órgão ou entidade.
- Colaboradores: São todos aqueles que possuem ou possuíram algum vínculo com a Acqio, funcionários, funcionários temporários, aprendizes, estagiários, prestadores de serviços, diretores, sócios, contratados, com vínculo ativo ou não (denominados ex) que têm, terão ou tiveram acesso às Informações da Acqio e/ou utilizaram, utilizam ou utilizarão sua infraestrutura tecnológica, mesmo após o término do regime contratual.
- Confidencialidade: garantir que somente pessoas autorizadas tenham acesso às informações e aos Ativos da Informação que necessitam no âmbito de suas atividades.
- Criptografia: é a prática de técnicas seguras para comunicação e armazenamento de informações, de modo que apenas os destinatários pretendidos possam acessar e compreender os dados.
- Alta Direção: Grupo formado pela presidência, diretoria e demais executivos;
- Disponibilidade: Princípio de Segurança da Informação, de garantia de acesso autorizado às informações e aos Ativos correspondentes sempre que necessário;

- Dispositivos móveis: Equipamentos de tecnologia da Informação que primam pela mobilidade física e que têm como características a capacidade de registro, armazenamento, transporte e/ou processamento de informações com a possibilidade de estabelecer conexões e interagir com outros sistemas e/ou redes. Estão enquadrados nesta categoria equipamentos, tais como, mas não limitado a: notebooks, laptops, PDAs, handhelds, celulares, smartphones, pendrives, cartões de memória, câmeras, tablets, entre outros;
- GMUD ou Gestão de mudanças: Processo que visa garantir que métodos e procedimentos padronizados sejam utilizados de forma eficaz em todas as atualizações/adequações necessárias no ambiente de tecnologia da Informação;
- Incidente de Segurança da Informação: qualquer evento ou ocorrência que comprometa a confidencialidade, integridade ou disponibilidade de dados, sistemas ou redes de informação em uma organização.;
- Integridade: Princípio de Segurança da Informação pelo qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- Prestadores ou Fornecedores: Pessoa física ou jurídica que presta serviços à Acqio.
- Segurança Cibernética: Prática de proteger sistemas, redes, dispositivos e programas contra ataques, danos, roubo ou acesso não autorizado. O objetivo da segurança cibernética é garantir a confidencialidade, integridade e disponibilidade das informações, bem como proteger os usuários e sistemas contra diversos tipos de ameaças cibernéticas.
- Segurança da Informação: Conjunto de processos e procedimentos que objetiva a preservação da confidencialidade, integridade, disponibilidade de dados e informações pertencentes à Acqio.
- Vulnerabilidades: Refere-se a uma fraqueza, falha ou inadequação em um sistema, aplicativo, rede ou processo que pode ser explorada por ameaças para comprometer a segurança da informação.

3. DIRETRIZES

A Acqio possui como objetivo desenvolver processos e produtos considerando os pilares e as boas práticas de segurança da informação, e, implementar controles e procedimentos para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

Esta Política segue orientada pelas diretrizes definidas pela Alta Administração da Acqio, baseadas nas normas, regulamentações e melhores práticas de mercado. Dessa forma, possui como diretrizes gerais:

- Buscar atender aos princípios de segurança da informação e comunicação:
  - Confidencialidade: garantir que a informação somente estará acessível para pessoas autorizadas;
  - Integridade: garantir que a informação, processada, armazenada ou transmitida, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não;
  - Disponibilidade: garantir que a informação estará disponível sempre que for necessário;
- Garantir que os sistemas e dados sob sua responsabilidade estejam devidamente protegidos e sejam utilizados apenas para o cumprimento de suas atribuições;
- Proteger os dados contra acessos indevidos, bem como contra modificação, destruição ou divulgação não autorizada;
- Assegurar que todas as informações sejam devidamente classificadas e recebam o nível de proteção adequada;
- Atender às leis e normas que regulamentam as suas atividades;
- Melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

Para cumprir as diretrizes acima, a Companhia adota os seguintes controles:

Classificação da Informação

Os tratamentos das Informações devem ser classificados de acordo com seu grau de sigilo e relevância, segundo os parâmetros delineados na Norma de Classificação da Informação, recebendo o devido tratamento visando permitir sua proteção durante todo o ciclo de vida.

Plano de Continuidade de Negócios

O Plano de Continuidade de Negócios da ACQIO tem o propósito de estabelecer diretrizes e responsabilidades, visando garantir a continuidade das operações vitais e preservar a integridade das informações processadas em momentos de interrupções e durante os processos de recuperação.

Gestão de Controles de Acesso

Visando garantir a segurança de sistemas e informações, a ACQIO possui normas e diretrizes especificas que tratam do controle de acesso, monitoramento do ambiente lógico e físico, de acordo com as melhores práticas de mercado e regulamentações vigentes.

As concessões de acesso devem ser distribuídas com base nas necessidades específicas de cada função, minimizando riscos de acesso indevido ou fraudulento. De forma similar, quando mudanças ocorrem, como transferências ou desligamentos, os acessos são revogados para manter a segurança dos ativos. Além disso, mantemos o procedimento de gerenciamento de senhas, com troca periodicaperiódica definida para minimizar riscos de acesso não autorizado.

Gestão de Armazenamento, Descarte, Destruição e Reutilização

Assegurar tratamento adequado a todas as informações, e garantir que sejam descaracterizadas ou destruídas de forma segura antes do descarte ou da reutilização. Essa abordagem é essencial para proteger a integridade dos dados e evitar que terceiros não autorizados tenham acesso às informações restritas, privadas ou confidenciais.

Gestão de Regras de Firewall

A Acqio tem suas diretrizes de Gestão de Regras de Firewall definidas em norma própria que estabelece as diretrizes para implantação das regras de firewall na Acqio, visando controlar o tráfego de rede, prevenir acessos não autorizados, proteger nossos ativos e informações sensíveis.

Gestão de Incidente de Segurança da Informação

A ACQIO possui uma abordagem proativa para garantir a segurança da informação no que diz respeito à gestão de incidentes. A Acqio adota as melhores práticas de mercado, permitindo que qualquer incidente de segurança da informação seja identificado, avaliado, registrado e tratado em tempo hábil conforme seu nível de criticidade, relevância e impacto, nos termos determinados no Plano de Resposta a Incidentes de Segurança. A pronta atuação na remediação, controle e retomada do ambiente afetado é essencial para minimizar os efeitos adversos nos negócios da Acqio.

Controles contra Malwares

Na Acqio os ativos são equipados com antivírus, monitorados e atualizados, para prevenção e detecção de software maliciosos em todos os Ativos de Tecnologia da Informação, e assim garantir a adesão e conformidade às práticas de segurança.

Hardening

Para mitigar riscos conhecidos de segurança, é fundamental implementar o conceito de Hardening, adotando as melhores práticas de segurança da informação e os padrões de mercado reconhecidos. Essas práticas estabelecem recomendações para a instalação, configuração e manutenção dos dispositivos móveis, com o objetivo de minimizar os riscos de falhas de segurança.

Gestão, Monitoramento e Controle de Logs

A Acqio realiza a gestão de conformidade com as melhores práticas de segurança e regulamentações vigentes, e para assegurar que existam trilhas de auditoria com nível de detalhamento suficiente para realizar o rastreamento de possíveis falhas e fraudes. A gestão e análise de logs são fundamentais para investigar e responder a incidentes de segurança, além de verificar se as regras de segurança são efetivas.

Criptografia

A Acqio incorpora controles criptográficos como uma parte essencial de sua estratégia de segurança da informação, buscando assegurar a confidencialidade, integridade e disponibilidade das informações. Nossos processos de criptografia seguem as melhores práticas da indústria, alinhando-se aos requisitos dos padrões PCI DSS e PCI PIN.

Desenvolvimento Seguro

Comprometidos com a qualidade e segurança de suas soluções, a Acqio baseia suas práticas no referencial da OWASP. Assim, A Acqio deve contar com norma especifica de Desenvolvimento Seguro, garantindo a adoção das melhores práticas para o desenvolvimento seguro de nossas aplicações.

Gestão de Mudanças

A Gestão de Mudança é um processo essencial que busca assegurar que todas as mudanças realizadas nos ambientes produtivos e de homologação sejam conduzidas de forma controlada e segura. Essas mudanças são avaliadas, planejadas, testadas, comunicadas, implementadas e documentadas, com o objetivo de mitigar os riscos envolvidos nas mudanças tecnológicas em ambientes operacionais.

Cópias de Segurança - Backup

As cópias de segurança, ou backups, são fundamentais para garantir a integridade e a disponibilidade das informações. As Informações relevantes da Companhia devem ser armazenadas de forma redundante para garantir a disponibilidade e restauração de arquivos digitais de computadores e sistemas corporativos de acordo com as normas vigentes.

Gestão de Ativos

Para garantir a proteção dos ativos, definimos os controles de segurança que devem ser implementados na Norma de Gestão de Ativos, para garantir o uso adequado ativos de informação.

Uso de Dispositivos e Tecnologias

São estabelecidas diretrizes fundamentais para a gestão e uso seguro dos dispositivos e tecnologias disponibilizadas aos Colaboradores, no desenvolvimento de suas atividades profissionais. Essas diretrizes têm como objetivo garantir a segurança da informação, protegendo os dados que são acessados, processados ou armazenados, de acordo com as melhores práticas do mercado.

Gestão de Capacidade

A Acqio adota práticas de monitoramento e otimização dos recursos disponíveis, com a cooperação entre a área de Diretoria de Tecnologia e as equipes de Infraestrutura e Segurança da Informação. Essa abordagem visa garantir o uso eficiente dos recursos e capacidade para atender ao desempenho requerido.

Gestão e Seleção de Fornecedores de Tecnologia e Segurança da Informação

A Acqio realiza a avaliação de seus fornecedores antes da contratação, com atenção especial àqueles que terão acesso a dados confidenciais, restritos, privados ou pessoais. Também são avaliados fornecedores que atuam em processos ou procedimentos críticos para as atividades operacionais da empresa, especialmente no que diz respeito à segurança da informação.

Proteção de Dados e Privacidade

A Acqio adota os mais modernos e eficazes padrões para a proteção dos dados pessoais que trata, mantendo seu Programa de Privacidade constantemente atualizado e em evolução. O uso desses dados é sempre realizado em conformidade com a LGPD e com a Política de Privacidade da empresa.

Auditoria e Conformidade

A Acqio é periodicamente submetida a auditorias que avaliam a conformidade de suas práticas com a Política de Segurança da Informação e Cibernética, bem como com suas demais políticas, normas internas e documentos de referência relacionados à segurança da informação e cibernética.

4. PAPEIS E RESPONSABILIDADES

4.1 Área de Segurança da Informação

A Área de Segurança da Informação da ACQIO é responsável por proteger os ativos da empresa e promover uma cultura de segurança sólida. Suas principais atribuições incluem a elaboração e atualização de políticas, promoção da melhoria contínua, programas de conscientização, alinhamento estratégico, integração de requisitos, gestão de resultados, manutenção de certificações (PCI DSS e PCI PIN), orientação aos colaboradores, prevenção e resposta a incidentes, controle de vulnerabilidades, gerenciamento de acessos, monitoramento de ativos e sincronização temporal, além da realização de auditorias e tratamento eficaz de incidentes.

4.2 Diretoria de Tecnologia

A Diretoria de Tecnologia da ACQIO é essencial para a eficiência operacional e o alinhamento estratégico da empresa. Entre suas responsabilidades estão: a gestão de compras de ativos tecnológicos, supervisão do processo de mudanças, projeção da capacidade dos sistemas, acompanhamento dos planos de continuidade e recuperação de desastres, administração de ativos com usuários finais e infraestrutura, elaboração e atualização do inventário de ativos, descarte seguro de informações, além da implementação de correções de segurança conforme orientações da área de Segurança da Informação.

4.3 Colaboradores

Todos os colaboradores da ACQIO têm um papel essencial na segurança da informação e cibernética, devendo seguir as normas e procedimentos estabelecidos, reportar incidentes e atividades suspeitas, participar de programas de conscientização, proteger os ativos de informação e manter a confidencialidade de suas credenciais de acesso. Esse comprometimento coletivo fortalece a cultura de segurança da empresa e contribui para sua resiliência frente às ameaças do cenário digital.

5. CONSIDERAÇÕES FINAIS

O descumprimento das diretrizes desta Política enseja a aplicação de medidas de responsabilização dos agentes que a descumprirem, conforme a Política Interna de Consequências.

Treinamento e Conscientização

Os Treinamentos constituem parte importante da construção de um ambiente cibernético seguro. O incentivo e a promoção de treinamentos e ações de conscientizações têm o objetivo de expandir a cultura de segurança da informação, e consequentemente, combater ameaças, vetores de exploração e interesses maliciosos.

Melhoria Contínua e Atualizações

A Acqio se empenha em promover a melhoria contínua de seus processos e procedimentos, utilizando como indicadores suas experiências e as tendências do mercado.

Reporte e Canais de Contato

Quaisquer violações desta Política deverão ser reportadas à Companhia por meio do Canal de Denúncias, disponível em https://acqio.com.br/denuncia/.

A Companhia garante a confidencialidade e anonimato das informações reportadas, bem como a não retaliação a denunciantes que estiverem agindo de boa-fé.

HISTÓRICO DE REVISÕES

Versão	Data de Revisão	Histórico da Revisão	Responsável
1.0	02/2024	Elaboração do documento	Área de Segurança da Informação
2.0	05/2025	Atualização do documento	Área de Segurança da Informação