POLÍTICA DE SEGURANÇA CIBERNÉTICA

Assunto: Resumo da Política de Segurança Cibernética	
Data de Emissão: 23/05/2022	**Data da Última atualização:** 23/05/2022

Política de Segurança Cibernética ("Política")

1. Introdução e Objetivo

A Política de Segurança Cibernética ("Política") assegura a preservação das informações geradas, adquiridas, processadas, armazenadas, transmitidas e descartadas; devendo ser prioridade constante da AZUMI DTVM LTDA. ("AZUMI"), reduzindo-se os riscos de falhas, os danos e/ou os prejuízos, e devem ser protegidas adequadamente; seguindo em conformidade com a Resolução nº 4.658, de 26 de abril de 2018; e Resolução nº 4.752, de 26 de setembro de 2019.

2. Abrangência

O público-alvo desta Política são todos os diretores e colaboradores da AZUMI, bem como estagiários e os prestadores de serviços, clientes e usuários dos produtos e serviços oferecidos pela instituição, a comunidade interna à sua organização e as demais pessoas que, conforme avaliação da instituição, sejam impactadas por suas atividades.

3. Diretrizes

Esta Política visa estabelecer as diretrizes a serem seguidas pela AZUMI se estendem da preservação das propriedades da informação, notadamente sua confidencialidade, integridade, disponibilidade e privacidade dos seus dados permitindo o uso e o compartilhamento da informação de forma controlada em nossos sistemas e informações prestadas, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

As diretrizes têm por principais objetivos:

- Tratamento confidencial: Informações Confidenciais recebidas são tratadas e arquivadas de forma segura e íntegra, se necessário com métodos de criptografia. Estas apenas serão acessadas por pessoas autorizadas e capacitadas para seu uso adequado; as informações somente serão fornecidas a terceiros, mediante autorização prévia do cliente ou para o atendimento de exigência legal ou regulamentar;

- Disponibilidade por necessidade: o uso de informações confidenciais será garantido apenas àqueles que tiverem acesso em vista de sua função ou que solicitarem sua divulgação por necessidade de trabalho, quando tal necessidade for concreta, sendo possível, desta maneira, identificar qual Colaborador detém cada tipo de informação ("as-needed");

- Integridade da informação: salvaguarda da exatidão e completeza da informação e dos métodos de processamento e arquivamento, protegendo as informações contra acesso, modificação, destruição ou divulgação não-autorizada.

- Legalidade de uso a informação: garantia de que a informação está em conformidade com a legislação em vigor. Cumprindo as leis e as normas que regulamentam os aspectos de propriedade e assegurar que os recursos colocados à sua disposição sejam utilizados apenas para as finalidades aprovadas pela empresa.

- Usuário: a política aplica-se a qualquer usuário da informação, incluindo qualquer Colaborador, incluindo empregados, contratados, estagiários, prestadores de serviços, parceiros que utilizam as informações da empresa.

4. Diretrizes Fundamentais desta Politica

Proteção da Informação.

As medidas de proteção da informação devem considerar:

- ✓ os níveis adequados de integridade, confidencialidade e disponibilidade;
- ✓ a legislação, as decisões judiciais, as diretrizes e as instruções e procedimentos em vigor;
- ✓ Manual de Compliance, em especial o Código de Ética;
- ✓ o alinhamento com as estratégias de cada área;
- ✓ as melhores práticas para a gestão da segurança da informação; e
- ✓ os aspectos comportamentais e tecnológicos

Responsabilidade pela Segurança da Informação

As atividades de Segurança da Informação são exercidas por pessoas com

sólidos conhecimentos em Segurança da Informação, inseridas na estrutura organizacional das áreas de Gestão de Riscos e Compliance.

Cada funcionário é responsável pela segurança da informação do grupo e deve cumprir as diretrizes, a declaração de princípios éticos e código de conduta e as instruções de procedimentos e restritos aplicáveis ás suas funções zelando pela correta aplicação das medidas de proteção.

Acesso à informação

O acesso e o uso de qualquer informação da empresa, pelo usuário, devem se restringir ao necessário para o desempenho de suas atividades profissionais no âmbito da AZUMI.

Para acessar informações nos sistemas da empresa deverão ser utilizadas somente ferramentas e tecnologias autorizadas pela empresa.

Senhas são pessoais e intransferíveis, não devem em hipótese alguma ser disponibilizadas a terceiros ou compartilhadas com outros colaboradores.

As Informações confidenciais poderão ser classificadas segundo seu grau de confidencialidade.

A segregação de acessos a informações confidenciais será estruturada a partir de grupos de perfil de acesso.

Regras fundamentais de segurança da informação

Dever de preservar. Os Colaboradores não devem transmitir nenhuma informação não-pública a terceiros. Todos os Colaboradores são responsáveis por preservar ativos de informação e devem estar comprometidos com a proteção adequada de informações e sistemas da empresa, considerando que a segurança da informação é um importante diferencial competitivo.

Autorização prévia. Toda e qualquer divulgação de informações estratégicas da empresa deve ser previamente autorizada.

Acesso privilegiado. Colaboradores da empresa deverão guardar sigilo sobre qualquer informação relevante à qual tenham acesso privilegiado, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento.

Operações em andamento. Colaboradores devem preservar a

confidencialidade de informações relativas a operações em andamento, bem como informações recebidas de entidades/pessoas cuja publicidade ou posição possa influenciar o mercado.

Divulgação acidental. Colaboradores devem evitar manter em suas mesas papéis e documentos confidenciais, e manter sigilo sobre senhas do computador, rede e sistemas. Funcionários e sócios devem garantir que o acesso à área de trabalho seja feito somente por pessoal autorizado.

Propriedade da informação. Toda informação produzida ou recebida pelos Colaboradores como resultado da atividade profissional ou dentro da empresa pertence ou foi cedido à AZUMI. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Propriedade de equipamentos. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da empresa, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta Política.

Autorização para gravação e uso. Esta Política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

Autorização para monitoramento de rede. O colaborador está ciente de que a AZUMI pode e monitorará a rede interna para garantir a integridade dos dados e programas.

Autorização para monitoramento mensagens. O colaborador está ciente de que a AZUMI pode e monitorará mensagens de e-mails ou qualquer outra forma de comunicação eletrônica a que o colaborador tiver acesso na empresa para garantir a integridade das informações e mensagens repassadas.

Usos inadequados. Toda tentativa de alteração dos parâmetros de segurança, por qualquer Colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição

cooperará ativamente com as autoridades competentes.

Dever de informar. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao Área de Tecnologia e ela, se julgar necessário, deverá encaminhar posteriormente à Diretoria de Compliance para análise.

Termo de confidencialidade

Todo Colaborador assinará o termo de confidencialidade de informações conforme o Anexo ao presente desta Política

5. Diligências e Controles

A AZUMI controla os dados, sistemas e serviços, com o objetivo de proteger os ativos de informações e a privacidade de seus clientes contra a coleta, retenção, uso, divulgação, modificação ou destruição não autorizada. Isso é abordado através de normas, procedimentos e arquitetura de segurança com a adoção de controles técnicos apropriados.

A política e os controles de segurança da informação fornecem cobertura de áreas críticas de segurança da informação, incluindo:

Programa de Conscientização de Segurança da Informação e Riscos Cibernéticos – Periodicamente é feito um programa de conscientização de segurança aos funcionários e demais colaboradores para que conheçam os riscos e possam agir adequadamente. As políticas de segurança garantem os deveres e responsabilidades dos funcionários e demais colaboradores em relação à proteção dos ativos de informação.

Controle de acesso - O acesso é concedido com um mínimo de privilégio e necessidade de saber. Todo o acesso é concedido com base em perfis de usuários e com aprovação prévia adequada na plataforma de Gerenciamento de Acessos. Acesso a dispositivos moveis e serviços de armazenamento web são controlados.

Segmentação dos Ambientes – Os ambientes são segregados para que exista um controle de tráfego entre eles, garantindo maior restrição nos ambientes que exigem mais integridade e confidencialidade.

Segurança de aplicações – Desde o processo de planejamento e criação da arquitetura, até o processo de implantação, as aplicações estão sujeitas a um processo de análise de segurança para confirmar que foram desenvolvidas de

acordo com nossas normas e padrões de segurança de desenvolvimento de aplicativos.

Classificação das Informações – Todas as informações geradas ou sobre custódia pela AZUMI, são classificadas de forma manual ou automática (quando possível) de acordo com as normas internas de classificação a informação, garantido o nível de proteção adequado a informação.

Plano de Continuidade ao Negócio e Recuperação de Desastres – O ambiente Operacional da AZUMI é digital, arquitetado para que os sistemas, processos e ativos críticos suportem eventos catastróficos utilizando de recursos em alta disponibilidade, garantindo contingência. Os sistemas que mantem essa disponibilidade são testados regularmente para garantir a eficácia do processo em casos reais de desastres. São feitas regularmente novas análises de impacto ao negócio e alterações no plano caso se façam necessários.

Gerenciamento de Fornecedores – O processo conduz análises de diligências em atividades relacionadas à Segurança da Informação e Compliance de terceiros, incluindo: avaliação de potenciais fornecedores para o cumprimento das políticas e controles da empresa; controles em relação a Privacidade dos Dados; revisões de devida diligência, incluindo a elaboração de classificações de risco e resultados; mitigação de riscos; Suporte na seleção de fornecedores.

Resposta a Incidentes – O departamento de Segurança da Informação detecta, controla e remedia incidentes relacionados a segurança de sistemas, processos e ativos de informação

Em caso de alguma violação, a equipe de segurança da informação tomará medidas para manter as informações seguras e mitigar a violação. As notificações oportunas de clientes afetados são emitidas de acordo com os requisitos contratuais, regulamentares e legislativos.

Periodicamente são feitas novas análises deste processo (plano) para garantir máxima eficiência na detecção e controle dos incidentes

Gestão de Vulnerabilidades – É feito regularmente processos de rotina que visem diminuir as falhas sistêmicas que possam ser exploradas por ataques. Todas as falhas detectadas são colocadas para acompanhamento e correção de acordo com o nível de criticidade do sistema.

Proteção de Recursos Computacionais – Todos os equipamentos computacionais da AZUMI, possuem políticas de configuração segura, atualizações constantes de patches de segurança e proteções contra malwares. Todos os tráfegos de rede e mídias removíveis são controlados e monitorados para detecção de incidentes.

Termo de confidencialidade

Todo Colaborador assina termo de confidencialidade de informações conforme o Anexo à presente Política.

6. Penalidades

O não cumprimento desta Política implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho e/ou de serviços, outra ação disciplinar e/ou processo civil ou criminal.

7. Manutenção dos Arquivos

A AZUMI manterá armazenado todos os arquivos eletronicamente, pertinentes ao processo de Conformidade (Compliance) desta Política pelo prazo mínimo de 05 (cinco) anos, conforme legislação vigente.

8. Controle de Revisão

A AZUMI manterá armazenado todos os arquivos eletronicamente, pertinentes ao processo de Conformidade (Compliance) desta Política pelo prazo mínimo de 05 (cinco) anos, conforme legislação vigente.

9. Vigência e Revisão Anual

A Política é revisada no mínimo, anualmente pela Instituição, podendo ser realizada em periodicidade menor, caso seja necessário, em decorrência de exigência regulamentar ou legislação aplicável, o qual será elaborada pela área de Compliance, mediante de acordo da Diretoria da Instituição.