POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO

CONTROLE DE APROVAÇÃO

ELABORAÇÃO	REVISÃO	APROVAÇÃO
Segurança da Informação Yago Martins	**Diretora de Compliance, Controles Internos e Riscos** Saul Barroso	**Diretor Controller** Eli Tassim

Sumário

PARTE I – IDENTIFICAÇÃO

1. OBJETIVO

A Política de Segurança da Informação estabelece diretrizes para garantir a confidencialidade, integridade e disponibilidade das informações da AZUMI, promovendo uma atuação segura, ética e legal de seus colaboradores.

Com base na Resolução nº 4.893/2021, na Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), junto a ISO/IEC 27001. A Política visa minimizar riscos, prevenir danos que possam comprometer a imagem e os objetivos da empresa e proteger dados pessoais de clientes, colaboradores e demais envolvidos.

Essa Política também define orientações para o uso seguro e ético dos recursos tecnológicos da AZUMI, assegurando conformidade com a legislação e boas práticas de segurança da informação.

2. ABRANGÊNCIA

Essa política aplica-se a diretores, gestores, colaboradores, estagiários, prestadores de serviços, parceiros, clientes, usuários e todas as partes impactadas pelas atividades da AZUMI. Incluindo terceiros e fornecedores que atuem em seu nome.

3. ALÇADA DE APROVAÇÃO

3.1. Segurança da Informação – Responsável pela elaboração

3.2. Diretor de Compliance, Controles Internos e Riscos – Responsável pela revisão

3.3. Diretor Controller – Responsável pela aprovação

4. RESUMO DA REVISÃO

28/05/2020 – Versão original.

09/02/2021 – Versão revisada

17/05/2022 – Versão revisada

31/05/2023 – Versão revisada

26/04/2025 – Versão revisada

26/01/2026 – Versão revisada

5. DOCUMENTOS E/OU INICIATIVAS DE REFERÊNCIA

- ABNT NBR ISO/IEC 27001 – Requisitos do Sistema de Gestão de Segurança da Informação – 2022;
- Código de Conduta Azumi.
- Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018)
- Resolução nº 4.893/2021 do Banco Central do Brasil (BC)

6. GLOSSÁRIO

- **Aplicação de Negócios:** Software ou programa desenvolvido internamente ou por parceiros de negócio ou prestadores de serviço, especialmente desenhados para automatizar ou apoiar processos de negócio da empresa.
- **Ferramenta de ITSM**: Canal de atendimento e registro de demandas de TI (Gerenciamento de Serviços de TI).
- **Colaboradores**: Todas as pessoas que atuam nas unidades e filais da AZUMI, ou seja, seus acionistas, conselheiros, diretores, gestores, colaboradores sob o regime CLT, estagiários, ou quaisquer pessoas que possam atuar em nome da AZUMI.
- **Confidencialidade:** Propriedade de manter a informação a salvo de acesso e divulgação não autorizados.
- **Conta de Acesso ou User ID**: Símbolo ou sequência de caracteres usados por um

sistema para identificar um usuário específico de forma a garantir sua unicidade.

- **Criptografia:** Ciência que se dedica a transcrever dados em cifras ou códigos que poderão ser, teoricamente, lidos apenas pelo destinatário da informação.

- **Disponibilidade:** Propriedade de manter a informação disponível para usuários autorizados, quando houver necessidade.

- **Gestor da Informação:** Responsável pela informação e medidas necessárias à segurança e controle efetivo do acesso à informação.

- **Incidente de Segurança**: Qualquer evento que resulte em perda ou danos aos ativos da Organização, ou qualquer ação que desrespeite as regras de segurança.

- **Informação Confidencial:** É uma informação sensível à estratégia ou aos negócios da AZUMI, e deve ser tratada com os mesmos requisitos de segurança das informações classificadas como ‘Restritas’.

- **Informação Interna:** É uma informação cujo conhecimento e uso está restrito ao ambiente interno da AZUMI, estando disponível a todos os colaboradores, bem como a fornecedores e prestadores de serviço que possuam cláusula de confidencialidade assinadas nos contratos de prestação de serviço.

- **Informação Pública**: Informação que pode e/ou deve ser divulgada para o público externo da AZUMI.

- **Informação Restrita:** É uma informação associada aos interesses estratégicos ou à cadeia de valor da AZUMI, sendo o acesso limitado a colaboradores devidamente autorizados.

- **Informação Sensível:** A informação é considerada sensível quando ela possui detalhes comerciais, operacionais, a reputação frente aos clientes, posição ou estratégia de mercado da AZUMI. Sua indisponibilidade, divulgação, alteração indevida, pode causar algum dano ou prejuízo à organização.

- **Integridade:** Propriedade de manter a informação exata, completa e atualizada.

- **Prestadores de Serviços**: Pessoa ou empresa que presta serviços à organização em atividades de curta ou média duração, incluindo consultores externos, terceiros,

auditores externos entre outros.

- **Segregação de funções (SOD Segregation Of Duties**): Consistem na separação entre pessoas distintas das atividades conflitantes de execução, autorização, aprovação, contabilização e controle, objetivando a redução da incidência de falhas ou fraudes, independente se sua estruturação é automática ou não.

- **Vírus:** Segmento de código ou programa que pode infectar replicar e se espalhar em sistemas computacionais sem a ação de um usuário.

PARTE II – CONTEÚDO

1. DIRETRIZES

Esta Política tem como objetivo estabelecer diretrizes para assegurar a prevenção, detecção e mitigação de riscos de segurança, abrangendo tanto o ambiente de computação em nuvem quanto a infraestrutura local da empresa, além dos recursos e informações da organização.

A segurança da informação é baseada nos três pilares fundamentais:

- **Confidencialidade:** Garantir que apenas pessoas devidamente autorizadas tenham acesso às informações.
- **Integridade:** Assegurar que apenas alterações, exclusões e adições autorizadas sejam realizadas nas informações, mantendo sua precisão e confiabilidade.
- **Disponibilidade:** Garantir que as informações estejam acessíveis para os usuários autorizados sempre que necessário.

A proteção das informações exige um gerenciamento eficiente e a implementação de medidas para prevenir ameaças como roubo, fraude, espionagem, perdas acidentais, incidentes cibernéticos e outros riscos.

O sucesso da Política de Segurança da Informação depende de uma abordagem integrada, que combina:

- Estrutura organizacional clara e bem definida, com responsabilidades atribuídas.

- Normas, Políticas e procedimentos atualizados e alinhados às melhores práticas de segurança.
- Proteção cibernética avançada, incluindo SOC, XDR, firewalls de próxima geração, IDS/IPS, antivírus, soluções de criptografia, detecção e resposta a incidentes.
- Treinamento e conscientização dos colaboradores sobre a importância da segurança da informação e comportamentos seguros, capacitando-os para identificar e prevenir potenciais ameaças.
- Mecanismos de controle eficazes para mitigação de riscos e monitoramento contínuo da infraestrutura.

Essa política reflete o compromisso da organização em proteger seus ativos de informação e garantir a segurança em todos os ambientes, sejam eles locais ou em nuvem.

2. RESPONSABILIDADES

2.1. TODOS OS COLABORADORES

- Adotar um comportamento seguro no uso de informações e recursos computacionais, reconhecendo que essa atitude é a primeira linha de defesa.
- Conhecer e seguir a Política de Segurança da Informação, agindo de forma coerente com suas diretrizes.
- Manter em sigilo suas identidades digitais e senhas, garantindo que sejam pessoais e intransferíveis. O compartilhamento de senhas é considerado falta grave e passível de sanções, conforme o Código de Conduta.
- Respeitar e preservar a confidencialidade, integridade e disponibilidade das informações da empresa, seus clientes, parceiros e fornecedores, mesmo após o término do vínculo contratual.
- Utilizar autorizações, informações e ativos fornecidos exclusivamente para as atividades designadas em suas funções ou atribuições.

- Comunicar qualquer suspeita de violação das regras de segurança ou comportamentos anormais, bem como acessos indevidos, à área de Segurança da Informação.
- Participar de programas de treinamento e conscientização sobre segurança da informação, contribuindo para a cultura de segurança organizacional.

2.2. GERENTES E DIRETORES

- Cumprir e garantir o cumprimento da Política de Segurança da Informação em todos os níveis de liderança, assegurando que suas equipes possuam acesso e conhecimento das diretrizes.
- Avaliar criteriosamente e autorizar solicitações de acesso às informações e recursos da empresa, garantindo que os colaboradores e terceiros tenham acesso somente ao que é necessário para suas funções.
- Informar imediatamente à área de TI, por meio da ferramenta de ITSM ou outro canal designado, qualquer troca de direitos de acesso, mudanças de função, transferências ou desvinculações, assegurando a revogação de acessos não mais necessários.
- Monitorar e comunicar riscos relacionados à segurança da informação à equipe responsável, bem como eventuais violações da política.
- Assegurar que todos os colaboradores sob sua gestão compreendam suas atribuições e responsabilidades relativas à segurança da informação.
- Estar atentos às diretrizes da política e aos riscos gerenciados pela equipe de segurança da informação, promovendo o uso adequado dos recursos e ativos de informação da empresa.

2.3. EQUIPES DE TI

- Garantir a disponibilidade, integridade e confidencialidade de todos os sistemas, dados e ativos de informação sob sua responsabilidade.

- Utilizar direitos de acesso privilegiado de forma responsável, profissional, ética, legal e aderente às diretrizes de segurança estabelecidas.
- Gerenciar o acesso lógico aos sistemas, garantindo que colaboradores tenham acesso apenas às informações e recursos previamente autorizados.
- Realizar backups antes de qualquer modificação em sistemas, documentando todas as alterações realizadas no ambiente de produção.
- Proibir a cópia de bases de dados do ambiente de produção para os ambientes de teste ou homologação sem a validação prévia da área de Segurança da Informação.
- Desativar imediatamente as identidades digitais e os acessos de ex-colaboradores ao término do vínculo empregatício ou contratual.
- Apoiar atividades de auditoria ou monitoramento relacionadas ao funcionamento ou configuração dos ativos, processos ou sistemas, incluindo contas de acesso, logs, configurações e eventos.
- Formalizar e reportar à área de Segurança da Informação qualquer risco identificado durante as atividades, especialmente os que não tenham sido adequadamente tratados ou reconhecidos pelos superiores ou demandantes.
- Implementar ou solicitar a implementação de controles apropriados para prevenir que registros sejam desativados, modificados ou apagados, ou que sistemas sejam utilizados de forma inadequada.

2.4. DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO

- Definir, documentar, publicar e manter atualizadas as políticas, normas e procedimentos relacionados à segurança da informação.
- Atuar proativamente na implementação e gestão de processos e ferramentas para mitigação de riscos cibernéticos, protegendo o ambiente computacional e as informações controladas pela empresa.
- Fornecer requisitos, controles e orientações sobre boas práticas de segurança da informação, incluindo:

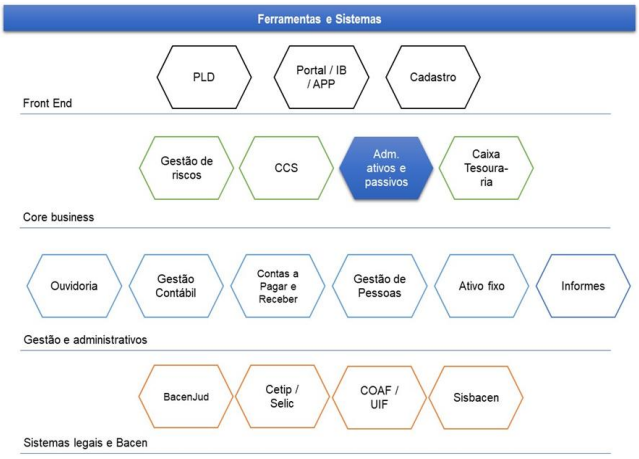
- Configuração segura de hardware, software e redes (incluindo redes wireless).
- Administração de contas de acesso.
- Aplicação de correções de Patches de segurança.
- Gestão de vulnerabilidades da Infraestrutura local e Nuvem
- Mapeamento e geração da Matriz de Risco da Empresa
- Ciclo de vida seguro no desenvolvimento de código.
- Tratamento e remoção de vírus ou malware.
- Liberação de acesso à navegação web (filtro de conteúdo).
- Participação em projetos e processos de TI ou negócios.
- Realização de Pentest e exercícios de Red Team
- Adequação e capacitação contínua da empresa em relação à Privacidade e Proteção de Dados, garantindo conformidade com a LGPD.
- Desenvolver, documentar e manter procedimentos de resposta e tratamento de incidentes de segurança da informação, assegurando abordagens eficientes para situações adversas.
- Estabelecer um plano integrado de gestão de riscos de segurança da informação, acompanhando e reportando seu progresso conforme objetivos acordados.
- Monitorar, cobrar e fiscalizar a revisão periódica de perfis de acesso pelos gestores e donos de processo.
- Disseminar conhecimento sobre práticas seguras para colaboradores e terceiros, promovendo conscientização e treinamento.
- Realizar testes e avaliações para medir a eficácia dos controles de segurança e treinamentos implementados.
- Avaliar e propor soluções para situações envolvendo segurança da informação que não estejam previstas na política vigente.
- Receber e tratar casos de violação das políticas de segurança, encaminhando-os às áreas pertinentes em alinhamento com o Código de Ética da empresa.

- Definir casos de aplicabilidade das políticas de segurança da informação que ainda estejam em fase de implementação por projetos específicos.

3. INFRAESTRUTURA DE TECNOLOGIA

3.1. ARQUITETURA DE SISTEMAS

O diagrama da arquitetura de sistemas e aplicativos implementados na AZUMI



Descrição das funcionalidades dos sistemas e aplicativos.

Serão implementados os sistemas e aplicativos dos principais fornecedores de serviços

- Plataforma SINQIA para a Controladoria e Custodia dos fundos de investimento, com a gestão dos ativos, desde o cadastro dos clientes e os lançamentos diários de pagamentos até o cálculo mensal das cotas dos fundos, que são dados que precisam ser registrados na Comissão de Valores Mobiliários (CVM) e fornecimento aos seus respectivos cotistas.

- Plataforma SINQIA para análise de passivo, amortizações, resgate e aportes em cotas. Emissão de relatórios e de solicitações de resgates, amortizações e aplicações em fundos de investimentos

- Sistema Fromtis (Fromtis Simple Solutions) para a checagem de custódia.

- Cadastro: KN-1 (Fornecedor: Advice) - Ferramenta que permite à instituição se instrumentalizar para criar e gerir o seu processo de Análise de Perfil de Investidor conhecido também como Suitability.

Os principais fornecedores e seus sistemas / aplicativos / serviços:

- Advice Informática Ltda. (Advice – PLD):

Sistemas: Aquilla e Risk

- Sinqia (SQControladoria, SQP-Custódia)

Sistemas: Ativo e Passivo

- Fromtis Serviços de Tecnologia Ltda. (Fromtis Simple Solutions)

Sistema: Fromtis – FIDC-Custódia

- Finaud Tec Soluções com Tecnologia Ltda.

Sistema: Risk Driver

- Central de Registro de Direitos Creditórios (CRDC).

Sistema: Checagem de lastro

- RTM – Rede de Telecomunicações para o Mercado Ltda.

Estrutura de backup site, Cloud Link e contingência física

- Integrador AZ Tech / Pluga Bank

Sistema: Bacenjud

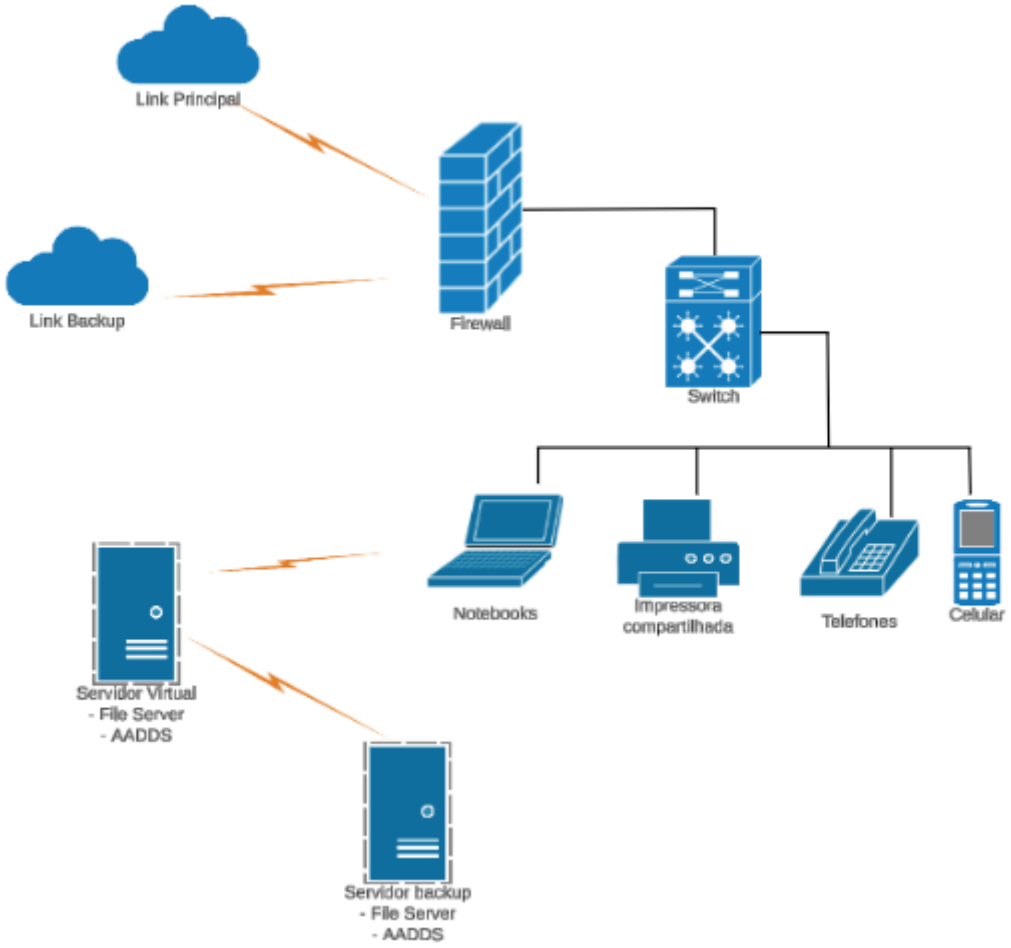
- Gopliance LTDA

Sistema de Gestão de Compliance

- Amazon AWS Serviços Brasil Ltda Servidores em nuvem: Controladoria, Fromtis (portal Fidic Custodia, Portal Fidic e 3040), Advice (Aquilla e Risk)

- Office 365 (Exchange Server, Sharepoint Server, Teams Server, Office)

3.2. ARQUITETURA DE REDE E INFRAESTRUTURA



Os sistemas e aplicativos estão em ambiente em “nuvem” (cloud) de fornecedores internacionais (Amazon, Microsoft).

A AZUMI contratou o servidor de contingência com replicação on-line (ambiente físico de contingência RTM);

A AZUMI realiza a auditoria de todos os logins administrativos dos Servidores Cloud e On-premise de 3 em 3 meses, também realizando a rotatividade das credenciais.

A instituição disporá de sólidos mecanismos que garantirão a privacidade, a integridade

e a disponibilidade das informações armazenadas. Esta garantia será obtida por meio de protocolos de acesso, controles estatísticos de uso e acesso, "firewalls", segurança física e lógica de aplicativos e de redes, "back-up" e contingência, todos normatizados por regras especialmente preparadas para este fim.

3.3. SEGURANÇA FÍSICA DO DATACENTER

Os recursos e processamento de instalações críticas para o negócio da instituição serão mantidos em áreas seguras, com barreiras de segurança apropriadas e recursos de controle de acesso.

a) O controle do acesso físico terá como objetivo proteger e evitar que pessoas estranhas tenham acesso às dependências nas quais são tratadas e/ou armazenadas as informações.

b) O Data Center, principal ambiente de tecnologia e informação, deverá abranger os seguintes recursos visando a segurança e a continuidade da operação de seus principais sistemas, como segue:

- Controle e monitoramento da temperatura e umidade do ar;
- Sistema automático de detecção e combate a incêndio;
- Cabeamento de rede de dados e energia embutidos (piso elevado);
- Pontos de energia distribuídos, aterrados e estabilizados;
- Nobreaks e gerador de energia com rotinas de manutenções preventivas;
- Proteção contra raios com revisão anual pelo departamento de Manutenção;
- Rede dos servidores certificada.

3.4. SEGURANÇA DOS SISTEMAS OPERACIONAIS

- Os sistemas operacionais Windows e Linux devem seguir as configurações recomendadas pelo CIS Benchmarks. Serão desativados serviços desnecessários e implementadas medidas de segurança (Hardening), conforme o Framework Global

- Todos os dispositivos e softwares utilizados na organização devem ser catalogados, monitorados e atualizados regularmente. A empresa realizará a remoção de software obsoleto, não autorizado ou não utilizado para garantir a conformidade com as políticas

de segurança

- Os logins serão permitidos exclusivamente dentro do território brasileiro. Qualquer acesso fora do Brasil será bloqueado automaticamente.
- Criação de conta de emergência para casos críticos e conta administradora de suporte para intervenção em máquinas.
- Acesso será configurado com acesso condicional no Azure, garantindo segurança e conformidade.
- Atualização do Windows será realizada em tempo real vinculada a política do ENTRA ID
- Conta administrador local será removida das máquinas para evitar privilégios indevidos.
- Desabilitação de painel de controle, PowerShell, CMD e instalações não autorizadas.
- Bloqueio de configurações das máquinas para prevenir alterações não autorizadas.
- A criptografia de disco local será aplicada a todos os dispositivos, protegendo dados em repouso e em trânsito.

3.5. VIGILÂNCIA ELETRÔNICA

A instituição realiza o monitoramento de suas dependências físicas por meio de câmeras de segurança (CFTV), com o objetivo de garantir a proteção dos colaboradores, visitantes, ativos físicos e das informações corporativas. O sistema de videomonitoramento opera de forma contínua, cobrindo áreas estratégicas e de acesso comum, respeitando os princípios da legalidade, necessidade e proporcionalidade previstos na Lei Geral de Proteção de Dados (LGPD).

As imagens capturadas são utilizadas exclusivamente para fins de segurança patrimonial e controle de acesso, sendo armazenadas em ambiente seguro e acessadas apenas por pessoal autorizado. O monitoramento não é realizado em áreas que comprometam a privacidade individual, como banheiros ou vestiários, assegurando o respeito à dignidade

e à privacidade dos colaboradores.

Esse controle contribui para a integridade do ambiente físico da instituição, promovendo um espaço mais seguro e alinhado com as diretrizes de governança e conformidade estabelecidas pela Política de Segurança da Informação.

Acesso e Responsabilidade: A gestão do sistema de CFTV, bem como a guarda das imagens capturadas, é de uso exclusivo da Companhia, sendo a gestão restrita a área de Risco e Compliance, não sendo permitido outras credenciais e/ou acessos similares.

Credenciais com Privilégios Administrativos: Controle das credenciais de administrador do sistema será mantido sob responsabilidade exclusiva do Diretor Compliance, em conjunto com o Diretor responsável no UNICAD BACEN (Operações).

Procedimentos para ocorrências e demandas Legais, deverá ser instituído um procedimento interno que regulamente:

• O tratamento de ocorrências internas que envolvam o uso das imagens de CFTV;

• O atendimento a solicitações provenientes de autoridades legais ou judiciais, com a devida atuação das áreas Jurídica, Segurança da Informação e Diretoria Executiva.

4. PROCEDIMENTOS DE SEGURANÇA

4.1. ACESSO LÓGICO E REMOTO

Todo acesso lógico ou remoto a sistemas será solicitado a área responsável. Qualquer acesso remoto solicitado por terceiros para manutenção em sistemas, só poderá ser liberado por meio de canal seguro de acesso mediante ao uso de VPN IPSEC Client-to-Site que será disponibilizado, instalado e configurado pela equipe de TI da AZUMI, estando sujeito ao monitoramento pelo administrador da rede.

4.2. INTERNET

Além das regras definidas, terá os seguintes controles de proteção:

- Firewall;

- Proteção Dia Zero
- Filtro de Aplicação
- Proteção contra Malware
- Webfilter
- Sandbox
- Email Protection
- MDR
- XDR
- NDR
- DLP
- VPN

4.3. SEGURANÇA DE USUÁRIOS

O acesso às informações da instituição será restrito aos colaboradores e prestadores de serviços que possuam justificativas válidas de negócio para execução de suas funções por meio de controles de autenticação e autorização.

- Senhas devem ter pelo menos 12 caracteres, com troca obrigatória a cada 90 dias.
- Senhas de administradores devem ter no mínimo 20 caracteres.
- Blacklist de senhas comuns, fracas e vazadas
- Bloqueio após 3 tentativas inválidas de login.

AUTENTICAÇÃO MULTIFATORIAL (MFA):

- MFA é obrigatória para todos os usuários, incluindo administradores.
- MFA expira a cada 15 dias, obrigando os usuários a se autenticarem novamente.

CONTROLE DE ACESSO E COMPORTAMENTO:

- Bloqueio por comportamento de risco, como tentativas de login anômalas.
- Desabilitação de credenciais não utilizadas por 20 dias.
- Conta de administrador será renomeada e restrita; privilégios elevados serão concedidos conforme necessidade específica.
- A partir das 20:00, o acesso a sistemas, softwares e infraestrutura Microsoft será bloqueado.

4.4. ANTÍVIRUS

A instituição adota o sistema Sophos como solução de segurança obrigatória para todas as máquinas e servidores, incorporando a tecnologia de Extended Detection and Response (XDR) para proteger contra vírus, malwares, spyware, trojans e outras ameaças cibernéticas.

O Sophos XDR garante a integridade das informações no ambiente de rede ao oferecer funcionalidades como detecção avançada de ameaças, respostas automatizadas, proteção contra ransomware, análise forense, prevenção de perda de dados (DLP) e gerenciamento de patches.

O sistema realiza atualizações automáticas e periódicas, com monitoramento contínuo e varreduras de hora em hora em todos os dispositivos conectados à rede, assegurando proteção proativa e mitigação de riscos em toda a infraestrutura da instituição.

4.5. GESTÃO DE VULNERABILIDADES

A instituição realiza a gestão de vulnerabilidades utilizando uma solução integrada entre as ferramentas Sophos e Tenable, garantindo uma abordagem robusta e eficiente para identificar, priorizar e remediar falhas de segurança. Essa integração permite:

Com a integração entre Sophos e Tenable, a instituição assegura um ciclo contínuo de identificação, análise, remediação e monitoramento das vulnerabilidades, fortalecendo a postura de segurança e minimizando os riscos associados a ameaças cibernéticas.

4.6. CONSCIENTIZAÇÃO E TREINAMENTO

A instituição realiza treinamentos regulares e programas de conscientização.

- **Conhecimento das políticas internas:** Orientação detalhada sobre as políticas de segurança da instituição, destacando responsabilidades e boas práticas para proteção da informação.
- **Identificação de ameaças:** Treinamento para reconhecer e responder a e-mails de phishing, links suspeitos, ataques de engenharia social e outros vetores de ameaça.
- **Engenharia social:** Capacitação para identificar e evitar manipulações que possam levar ao vazamento de informações sensíveis ou ao acesso indevido a sistemas.
- **Proteção de dados sensíveis:** Orientação sobre a importância da confidencialidade, integridade e disponibilidade das informações, além de diretrizes para o manuseio seguro de dados críticos.
- **Criação e gestão de senhas seguras:** Instruções sobre como criar senhas fortes e únicas, bem como a importância de armazená-las de forma segura, utilizando ferramentas confiáveis, como gerenciadores de senhas.

4.7. EM RELAÇÃO AO USO E TRANSPORTE DO EQUIPAMENTO

- Mantenha o equipamento sempre com você
- Atenção em saguões de hotéis, aeroportos, aviões, táxi etc
- Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível
- Atenção ao transportar o equipamento na rua
- Não se conecte em redes wi-fi públicas (restaurantes, aeroportos, parques etc.), sem uso de VPN
- Ao se conectar na sua residência, juntamente com uso da VPN, garanta que seu roteador esteja com a senha de administrador diferente da fornecida pelo fabricante.

Além disso, verifique com o fornecedor da rede wi-fi a aplicação de configurações de segurança como, por exemplo: habilitação do protocolo WPA2

4.8 EM CASO DE FURTO OU ROUBO

- Registre a ocorrência em uma delegacia de polícia
- Comunique rapidamente ao seu superior imediato e as áreas de Segurança da Informação e Tecnologia da Informação;
- Envie uma cópia da ocorrência para a área de Tecnologia da Informação.

5. PENALIDADES

- Qualquer colaborador deve comunicar imediatamente a Área de Segurança da Informação caso identifique a violação desta política ou demonstração de conduta que ameace a proteção do ambiente, colaborativo dos sistemas, dos processos ou dos recursos computacionais da AZUMI, seja de forma maliciosa ou não intencional
- Descumprimentos das diretrizes de segurança da AZUMI são passiveis de punição. Os procedimentos definidos no Código de Conduta devem ser aplicados nestas ocorrências
- As ocorrências de violação de regras não contempladas no Código de Conduta são passiveis de medidas educativas alinhadas com o superior imediato do colaborador ou gestor do contrato em questão.

6. INFORMAÇÕES SOBRE O DOCUMENTO

1. Periodicidade de revisão desse Documento.	(x) 1 ano ( ) 2 anos ( ) 3 anos	() Periodicidade prevista em regulamentação (x) Periodicidade definida internamente

2. Necessidade de divulgação do documento no site da internet da AZUMI DTVM	( ) Sim (x) Não	
3. Documento é para atendimento de regulamentação(ções) específica(s)	( ) Sim (x) Não	Resolução nº 4.893/2021 Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) ISO/IEC 27001