AUCBA
ASSOCIAÇÃO UNIVERSITÁRIA
E CULTURAL DA BAHIA

POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

POLÍTICA
INSTITUCIONAL
Nº1 - v2

POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

Maio de 2023

SUMÁRIO

1. INTRODUÇÃO

1.1. A ASSOCIAÇÃO UNIVERSITÁRIA E CULTURAL DA BAHIA – AUCBA, mantenedora da Universidade Católica do Salvador - UCSAL tem como missão “Promover e manter obras educativas e culturais com qualidade, sustentabilidade e inspiração humanista-cristã”.

1.2. A AUCBA entende que a informação corporativa é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos produtos ofertados a seus clientes.

1.3. A AUCBA compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

1.4. Dessa forma, a AUCBA estabelece sua Política Geral de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

2. PROPÓSITO

2.1. Esta política tem por proposito estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores e parceiros da AUCBA adotar padrões de comportamento seguro, adequados às metas e necessidades da AUCBA.

2.2. Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação.

2.3. Resguardar as informações da AUCBA, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade.

2.4. Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus colaboradores, clientes e parceiros.

2.5. Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da AUCBA como resultado de falhas de segurança.

3. ESCOPO

3.1. Esta política considera a abrangência da segurança da informação nos aspectos físico, lógico e comportamental, preservando a confidencialidade, integridade e disponibilidade das informações da AUCBA.

3.2. Esta política se aplica a todos os usuários da informação da AUCBA, incluindo qualquer indivíduo ou organização que possui vínculo com a AUCBA, tais como colaboradores, ex-colaboradores, prestadores de serviço e ex-prestadores de serviço, que possuíram, possuem ou virão a possuir acesso às informações da AUCBA e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura da AUCBA.

4. DIRETRIZES

4.1. O objetivo da gestão de Segurança da Informação da AUCBA é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos na instituição.

4.2. A Mantenedora e o Comitê Gestor de Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação na AUCBA. Desta forma, adotam todas as medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades da AUCBA.

4.3. É política da AUCBA:

4.3.1. Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação da AUCBA sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;

4.3.2. Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: Colaboradores, parceiros e, onde pertinente, clientes;

4.3.3. Garantir a educação e conscientização sobre as práticas adotadas pela AUCBA de segurança da informação para Colaboradores, parceiros e, onde pertinente, clientes;

4.3.4. Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

4.3.5. Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;

4.3.6. Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;

4.3.7. Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

5. PAPÉIS E RESPONSABILIDADES

5.1. Comitê Gestor de Segurança da Informação – CGSI:

5.1.1. Fica constituído o Comitê Gestor de Segurança da Informação - CGSI, contando com a participação de um representante da Mantenedora e um membro das seguintes áreas: Reitoria, Tecnologia da Informação, Recursos Humanos, Jurídico e Comunicação, Registro Acadêmico.

5.1.2. O Comitê Gestor de Segurança da Informação – CGSI será presidido pelo membro da Mantenedora, responsável pelas convocações ordinárias e extraordinárias dos demais membros.

5.1.3. É responsabilidade do CGSI:

5.1.3.1. Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;

5.1.3.2. Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;

5.1.3.3. Garantir que as atividades de segurança da informação sejam executadas em conformidade com o CGSI;

5.1.3.4. Promover a divulgação do CGSI e promover as ações necessárias para disseminar uma cultura de segurança da informação no ambiente da AUCBA.

5.2. Coordenação de Tecnologia da Informação:

5.2.1. É responsabilidade da Coordenação de Tecnologia da Informação:

5.2.1.1. Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções do CGSI;

5.2.1.2. Apoiar o CGSI em suas deliberações;

5.2.1.3. Elaborar e propor ao CGSI as normas e procedimentos de segurança da informação, necessários para se fazer cumprir a PGSI;

5.2.1.4. Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

5.2.1.5. Tomar as ações cabíveis para se fazer cumprir os termos desta política;

5.2.1.6. Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

5.3. Gestores da Informação:

5.3.1. É responsabilidade dos Gestores da Informação:

5.3.1.1. Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pela AUCBA;

5.3.1.2. Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela AUCBA;

5.3.1.3. Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas conforme necessário;

5.3.1.4. Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

5.3.1.5. Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela AUCBA.

5.4. Usuários da Informação:

5.4.1. É responsabilidade dos Usuários da Informação:

5.4.1.1. Ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

5.4.1.2. Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas e procedimentos à Coordenação de Tecnologia da Informação ou, quando pertinente, ao Comitê Gestor de Segurança da Informação;

5.4.1.3. Comunicar à Coordenação de Tecnologia da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da AUCBA;

5.4.1.4. Assinar o Termo de Uso de Sistemas de Informação da AUCBA, formalizando a ciência e o aceite integral das disposições da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

5.4.1.5. Responder pela inobservância da Política Geral de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

6. SANÇÕES E PUNIÇÕES

6.1. As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa.

6.2. A aplicação de sanções e punições será realizada conforme a análise do Comitê Gestor de Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o CGSI, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

6.3. No caso de terceiros contratados ou prestadores de serviço, o CGSI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato.

6.4. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a AUCBA, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens 6.1, 6.2 e 6.3 desta política.

7. CASOS OMISSOS

7.1. Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação.

7.2. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da AUCBA adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações da AUCBA.

8. GLOSSÁRIO

a) **Ameaça**: Causa potencial de um incidente, que pode vir a prejudicar a AUCBA.

b) **Ativo:** Tudo aquilo que possui valor, para a AUCBA, tais como bens e direitos.

c) **Ativo de informação:** Patrimônio intangível da AUCBA, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a AUCBA por parceiros, clientes, colaboradores e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da AUCBA ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

d) **Comitê Gestor de Segurança da Informação – CGSI:** Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria da AUCBA, que tem por finalidade tratar questões ligadas à Segurança da Informação.

e) **Confidencialidade:** Propriedade dos ativos da informação da AUCBA, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

f) **Controle:** Medida de segurança adotada pela AUCBA para o tratamento de um risco específico.

g) **Disponibilidade:** Propriedade dos ativos de informação da AUCBA, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.

h) **Gestor da Informação:** Usuário da informação que ocupe cargo especifico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

i) **Incidente de segurança da informação:** Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da AUCBA.

j) **Integridade:** Propriedade dos ativos da informação da AUCBA, de serem exatos e completos.

k) **Risco de segurança da informação:** Efeito da incerteza sobre os objetivos de segurança da informação da AUCBA.

l) **Segurança da informação:** A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da AUCBA.

m) **Usuário da informação:** Colaboradores com vínculo empregatício de qualquer área da AUCBA ou terceiros alocados na prestação de serviços a AUCBA, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizados a utilizar manipular qualquer ativo de informação da AUCBA para o desempenho de suas atividades profissionais.

n) **Vulnerabilidade:** Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da AUCBA.

9. REVISÕES

9.1. Esta política é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

9.2. Histórico de Revisões:

9.2.1. Versão Inicial: Abril de 2022.

9.2.2. Versão Atual: Maio de 2023

10. GESTÃO DA POLÍTICA

10.1. A Política Geral de Segurança da Informação é aprovada pelo Comitê Gestor de Segurança da Informação-CGSI, em conjunto com a Diretoria da AUCBA.


AUCBA
ASSOCIAÇÃO UNIVERSITÁRIA
E CULTURAL DA BAHIA