Política Geral de Segurança da Informação

Sumário

1. INTRODUÇÃO

1.1. A CYA entende que a informação corporativa é um bem essencial para suas atividades.

1.2. A CYA compreende que a manipulação de sua informação e/ou de seus CLIENTES passa por diferentes meios de armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

1.3. A CYA utiliza metodologias de Gestão de Riscos, Gestão de Vulnerabilidades, Gestão de Incidentes, Planos de Resposta a Incidentes e Campanhas de Conscientização parara que os objetivos de proteção da informação sejam alcançados e estabelece o uso aceitável dos recursos de forma que seus colaboradores e/ou prestadores de serviço consigam exercer suas funções.

1.4. A CYA utiliza mecanismos, ferramentas e serviços de fabricantes mundialmente reconhecidos e certificados nos mais diversos padrões de segurança para suportar sua estratégia de Segurança da Informação.

1.5. Dessa forma, a CYA 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 CYA e/ou de seus CLIENTES.

2. PROPÓSITO

2.1. Esta política tem por propósito estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores e/ou prestadores de serviço da CYA adotar padrões de comportamento seguro, adequados às metas e necessidades da CYA;

2.2. Orientar quanto à adoção de controles e processos para atendimento dos requisitos para segurança da informação;

2.3. Resguardar as informações da CYA e/ou de seus CLIENTES, garantindo requisitos adequados de confidencialidade, integridade, disponibilidade e privacidade;

2.4. Prevenir possíveis causas de incidentes e responsabilidade legal da CYA;

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 CYA como resultado de falhas de segurança.

3. ESCOPO

3.1. Esta política se aplica a todos os colaboradores e/ou prestadores de serviços da CYA.

4. DIRETRIZES

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

4.2. A Diretoria e o Comitê Gestor de Segurança da Informação estão comprometidos com uma gestão efetiva de segurança da informação na CYA. Desta forma, adotam todas 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 as necessidades da CYA.

4.3. É política da CYA:

4.3.1. Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos adequados de confidencialidade, integridade, disponibilidade e privacidade das informações da CYA e de seus CLIENTES 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.

4.3.3. Garantir a educação e conscientização sobre as práticas adotadas pela CYA de segurança da informação.

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 eles 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 resposta a incidentes.

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. COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A CYA comunicará à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados a ocorrência de incidente de segurança, que possa acarretar risco ou dano relevante aos titulares.

A referida comunicação deverá ser feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I. a descrição da natureza dos dados pessoais afetados;

II. as informações sobre os titulares envolvidos;

III. a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV. os riscos relacionados ao incidente;

V. a causa do incidente;

VI. o impacto do incidente;

VII. os motivos da demora, no caso de a comunicação não ter sido imediata; e

VIII. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

6. PAPÉIS E RESPONSABILIDADES

6.1. **COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO**

6.1.1. É responsabilidade do COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO:

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

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

6.1.1.3. Garantir que as atividades de segurança da informação sejam executadas em conformidade com a Política Geral de Segurança da Informação;

6.1.1.4. Promover a divulgação das Políticas de Segurança da Informação e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente da CYA.

6.2. **DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO**

6.2.1. É responsabilidade do departamento de Segurança da Informação:

6.2.1.1. Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções do Comitê Gestor de Segurança da Informação;

6.2.1.2. Apoiar o Comitê Gestor de Segurança da Informação em suas deliberações;

6.2.1.3. Elaborar e propor ao Comitê Gestor de Segurança da Informação as normas e procedimentos de segurança da informação, necessários para se fazer cumprir a Política Geral de Segurança Informação;

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

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

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

6.3. **GESTORES DA INFORMAÇÃO**

6.3.1. É responsabilidade dos Gestores da Informação:

6.3.1.1. 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 CYA;

6.3.1.2. Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação delas conforme necessário;

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

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

6.4. **DEPARTAMENTO DE RECURSOS HUMANOS**

6.4.1. É responsabilidade do departamento de Recursos Humanos:

6.4.1.1. Suportar a criação do código de ética e conduta da CYA;

6.4.1.2. Auxiliar na disseminação da cultura de Segurança da Informação;

6.4.1.3. Suportar a definição e execução de ações disciplinares aplicadas pela CYA.

6.5. **GESTORES E COORDENADORES**

6.5.1. É responsabilidade dos gestores e coordenadores:

6.5.1.1. Solicitar a equipe de tecnologia da informação a concessão de acesso a novos colaboradores ou colaboradores que necessitem de novos acessos conforme mudanças em suas atividades laborais;

6.5.1.2. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão;

6.5.1.3. Auxiliar na disseminação da cultura de Segurança da Informação.

6.6. **DEPARTAMENTO JURÍDICO**

6.6.1. É responsabilidade do departamento jurídico:

6.6.1.1. Acompanhar eventuais alterações legais e/ou regulatórias;

6.6.1.2. Incluir nos contratos cláusulas específicas relacionadas à segurança da informação;

6.6.1.3. Tomar as providências jurídicas cabíveis em casos de incidentes;

6.6.1.4. Garantir que as bases legais utilizadas no tratamento de dados pessoais estejam de acordo com a legislação.

6.7. **TECNOLOGIA DA INFORMAÇÃO**

6.7.1. É responsabilidade da gerência de tecnologia da informação:

6.7.1.1. Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para colaboradores e/ou prestadores de serviços;

6.7.1.2. Conceder, quando autorizado, o acesso aos colaboradores e/ou prestadores de serviços, conforme indicado pelos gestores da informação;

6.7.1.3. Revogar, quando solicitado, o acesso dos colaboradores e/ou prestadores de serviço, conforme indicado pelos gestores da informação;

6.7.1.4. Apoiar a revisão periódica da validade de credenciais de acesso dos colaboradores e/ou prestadores de serviço fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação;

6.7.1.5. Executar procedimentos de descarte de informações ao término da vida útil dos ativos no âmbito tecnológico, utilizando as boas práticas e técnicas que tornem as informações originais irrecuperáveis;

6.7.1.6. Preparar e manter o inventário dos equipamentos fornecidos pelo CYA aos seus colaboradores para o desempenho de suas atividades segundo as normas definidas pela Gerência de Segurança da Informação;

6.7.1.7. Documentar e monitorar todas as contas bem como analisar atividades suspeitas reportada pelas ferramentas disponíveis;

6.7.1.8. Implementar e manter os controles de segurança definidos pela Gerência de Segurança da Informação no âmbito tecnológico;

6.7.1.9. Durante o desligamento de colaboradores CYA revogar as contas de acesso;

6.7.1.10. Auxiliar na disseminação da cultura de Segurança da Informação.

6.8. **USUÁRIOS DA INFORMAÇÃO**

6.8.1. É responsabilidade dos Usuários da Informação:

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

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

6.8.1.3. Comunicar à Gerência de Segurança 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 CYA.

7. SANÇÕES E PUNIÇÕES

7.1. As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança poderão acarretar medidas disciplinares cabíveis, dentre elas:

- Orientação;
- Advertência Verbal;
- Advertência por escrito;
- Suspensão;
- Demissão sem justa causa;
- Demissão por justa causa.

7.2. A medida disciplinar adotada deverá ser razoável e proporcional à falta cometida, sendo aplicada o mais rapidamente possível. Permite-se um período maior para a aplicação de medidas quando a falta requerer apuração dos fatos e das devidas responsabilidades. Violações semelhantes devem receber sanções semelhantes.

8. CASOS OMISSOS

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

9. REVISÕES

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

10. COMPROMETIMENTO DA ALTA DIREÇÃO

10.1. A Diretoria da CYA , ao aprovar esta Política Geral de Segurança da Informação, institui um compromisso para com a melhoria contínua dos procedimentos relacionados com a segurança da informação, buscando sempre manter a CYA em conformidade com normas legais e regulamentares sobre os referidos temas, guiada pelos princípios, conceitos, valores e práticas aqui adotados, com o objetivo de assegurar a confidencialidade, a integridade e a disponibilidade dos dados da CYA ou por ela controlados e dos sistemas de informação por ela utilizados, permitindo à instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

11. GESTÃO DA POLÍTICA

11.1. A Política Geral de Segurança da Informação é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria da CYA.

11.2. A presente política foi aprovada no dia 12 de março de 2021.