POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

1. Objetivo

A informação é um dos patrimônios mais importantes a ser preservado pela Instituição. Assim, o Grupo Bexs estabelece a presente Política, a fim de orientar e garantir a aplicação das diretrizes estratégicas e princípios para proteção dos ativos tangíveis e intangíveis da Instituição, dos clientes e interesses do público em geral. Ainda, é objetivo deste normativo atender às leis e normas regulamentadoras do mercado, principalmente no tocante a Resolução CMN nº 4.893/2021 do Banco Central do Brasil, fazendo com que se torne parte da cultura de segurança cibernética, por meio de programas de capacitação, prestação de informações à clientes e usuários sobre precaução na utilização de produtos e serviços e o comprometimento da Alta Administração com a melhoria contínua dos procedimentos.

2. Público – Alvo

Está Política visa atender o público geral, especialmente clientes e parceiros, administradores, gestores, colaboradores, estagiários e prestadores ou fornecedores de serviços que se relacionam com o Grupo Bexs, direta ou indiretamente.

3. Procedimentos e Controles

As violações das Políticas e procedimentos de segurança do Grupo Bexs, após apuração e constatação de responsabilidades, poderão desencadear ações disciplinares, rescisão de contrato de trabalho e medidas administrativas/judiciais cabíveis.

4. Compromisso de Sigilo e Confidencialidade

Terceiros e parceiros deverão assumir o dever de sigilo, por si, seus empregados, prepostos ou terceiros sob suas ordens e efetuar uso, com prévia autorização, das informações críticas sobre todos os processos de negócio do Grupo Bexs, ainda que em caso de rescisão contratual.

5. Contratação de Fornecedores e Prestadores de Serviços

A contratação de fornecedores deverá observar diretrizes internas, a fim de assegurar a contratação de fornecedores parceiros idôneos, de boa conduta social, ambiental e ética, que incentivem a adoção de boas práticas, bem como contratar bens e serviços por preços coerentes praticados pelo mercado.

Caso o serviço a ser contratado utilize armazenamento de dados relevantes em nuvem, após procedimento interno de averiguação, deverá haver a comunicação ao Banco Central do Brasil, em até dez dias após a contratação dos serviços.

Ainda, nos casos de inexistência de convênio para troca de informações entre o Banco Central do Brasil e às autoridades supervisoras dos países onde os serviços poderão ser prestados, o Compliance deverá solicitar autorização do Banco Central do Brasil, no prazo mínimo de (60) sessenta dias antes do início da contratação.

6. Proteção contra Vírus e *Softwares* Maliciosos

Servidores, estações de trabalho ou notebook, deverão ser protegidos por *software* de *antimalware*, homologado pela Instituição. As estações de trabalho serão gerenciadas pelos administradores, impossibilitando que o colaborador desabilite os *softwares* de proteção.

7. Cópia de Segurança (*backup*)

A área de Tecnologia da Informação realizará controle de *backup*, estabelecendo dados a serem copiados e a periodicidade de retenção, a fim de garantir a recuperação em caso de falha ou desastre e ainda atender requisitos legais e fiscais. O armazenamento deverá ser efetuado com a identificação de cada mídia, data do *backup* e tempo de retenção.

8. Criptografia

As informações confidenciais internamente tratadas são armazenadas e trafegadas de forma criptografada, conforme nível de criticidade e confidencialidade definidos nos documentos de classificação da informação.

9. Uso da Rede Corporativa

Os usuários autorizados possuem acesso à rede corporativa para disponibilidade e armazenamento de arquivos pertinentes ao negócio, devendo o acesso ser tratado conforme classificação de informação e não como informação particular. O acesso deverá ser realizado de forma a atender normas internas.

10. Monitoramento

Com objetivo de identificar atividades não autorizadas, os sistemas e recursos de rede são monitorados e os eventos de segurança analisados.

11. Controle de Acesso

O acesso a informações, serviços de rede e aplicações são controlados visando evitar o acesso indevido. Existem regras para controle de acesso, considerando as permissões de acordo com a sensibilidade da informação. O Grupo Bexs possui procedimentos formais, que são passíveis de controle e auditoria. Toda violação de acesso identificada deve ser registrada e analisada pelas áreas responsáveis.

12. Gerenciamento de Senhas de Acesso/Acessos aos Sistemas da Empresa por Fornecedores

A senha de autenticação é a forma de certificar a identificação do usuário (*login*) e consequentemente atribuir direitos de acesso aos recursos e sistemas aplicativos autorizados. Quando identificada a necessidade de intervenção do fornecedor, o acesso de terceiros será controlado ostensivamente, com objetivo de manter o controle do console para as duas extremidades.

13. Aquisição, Desenvolvimento e Manutenção dos Sistemas de Informação

Todo o desenvolvimento dos sistemas de informação deverá seguir a metodologia adotada pelo Grupo Bexs. Aquisições, desenvolvimentos ou manutenções de sistemas de informação, deverão ser considerados os requisitos especiais de segurança. O processo deverá possuir documentação técnica e operacional, para criar base de conhecimento e melhor controle dos sistemas utilizados.

14. Controle de Implementações e Mudanças Operacionais

Toda alteração em ambiente de produção deverá ser planejada e homologada.

15. Gestão de Vulnerabilidades

Os procedimentos e controles adotados para reduzir a vulnerabilidade dos incidentes na Instituição e demais quesitos, determinam a necessidade de adoção de diretrizes para correção de fragilidade das aplicações de *hardenings* e *patches* de segurança, que deverão ser instalados em todos os componentes de sistema, estações de trabalho, servidores e/ou dispositivos de rede adotados pela Instituição.

Deverão ser consideradas como críticas, *patches* e correções de segurança para vulnerabilidades, considerando a seguinte classificação: **a**) urgente; **b**) crítica; **c**) alta.

16. Resposta a Incidentes de Segurança

A resposta aos incidentes deverá ser tratada de forma a limitar os danos e minimizar o tempo e os custos de recuperação, que envolve um método organizado para lidar com as consequências de um ataque contra a segurança de um sistema computacional.

A implementação deste processo será de responsabilidade da equipe de resposta a incidentes, ou **CSIRT** (*Computer Security Incident Response Team*), formada por analistas de segurança e representantes legais.

O processo de resposta aos incidentes de segurança compreende: detecção, triagem e análise, mitigação, investigação, resposta e educação. As tratativas dos incidentes deverão ocorrer, ressalvadas as características principais e considerando os quesitos de origem, vulnerabilidade, criticidade, impacto e ativo alvo. Não obstante, deverão ser observados os tipos de severidade - média e baixa, alta ou severidade crítica.

17. Compartilhamento de Informações sobre os incidentes relevantes

Exceto em casos que exigem sigilo de informações estratégicas para o negócio, será adotado o padrão de soluções de ferramentas disponibilizadas ou sugeridas pelas associações das quais o Grupo Bexs faz parte, para que o compartilhamento de incidentes seja eficiente e garanta a assimilação do processo.

18. Continuidade de Negócios

Os procedimentos e a metodologia adotados pela Instituição serão base para as simulações de teste de continuidade de negócio, a fim de garantir a confidencialidade, integridade e disponibilidade dos serviços contratados em nuvem. Neste sentido, as áreas de Tecnologia e Segurança da Informação deverão garantir a continuidade e recuperação nos serviços de nuvem contratados, além do gerenciamento das interrupções que possam ocorrer.

Ainda, deverão ser consideradas opções de portabilidade, para assegurar que os negócios não dependam de provedor único, com objetivo de evitar aprisionamento tecnológico ou dependência de fornecedores e eventuais custos que sobreponham à troca de fornecedor ou tecnologia empregada.

19. Conformidade

Visando assegurar a inexistência de irregularidades nas atividades executadas pelo Grupo Bexs, deverão ser tomados os devidos cuidados para atendimento à conformidade com os requisitos de negócio, leis civis, contratuais e regras de segurança.

20. Campanhas de Conscientização de Segurança

O Grupo Bexs, periodicamente, proverá treinamento de conscientização de segurança aos colaboradores, com apoio e envolvimento da Alta Administração.

Assim como a divulgação periódica de informes, com o objetivo de disseminar e aculturar todos os colaboradores da instituição, quanto a diretrizes de Segurança da Informação.

21. Comunicação

Quaisquer indícios de irregularidades no cumprimento das determinações desta Política serão alvo de investigação interna e devem ser comunicadas imediatamente ao Departamento de Segurança da Informação, através do *e-mail*: csirt@bexsbanco.com.br