Banco Caixa Geral Brasil

Política de Segurança Cibernética

Abril/2021

SUMÁRIO

1. INTRODUÇÃO

A Política de Segurança Cibernética é o documento que orienta sobre as responsabilidades do BCG-Brasil para cumprimento dos requisitos das Resoluções 4.658 e 4.752 (Resolução 4.893 a partir de julho/21) do Banco Central do Brasil.

2. OBJETIVO

O objetivo desta política é orientar os colaboradores e definir os procedimentos e controles do BCG-Brasil em relação à segurança cibernética, os requisitos mínimos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, estando em conformidade com a legislação vigente.

Destaca-se que além dos fornecedores de nuvem, os fornecedores de tecnologia da informação devem estar em conformidade com esta Política.

3. ABRANGÊNCIA

Esta Política Corporativa submete principalmente à área de Segurança da Informação e a todos os administradores e demais colaboradores do Banco Caixa Geral - Brasil S.A., doravante denominado BCG-Brasil, com a recomendação de serem diligentes no cumprimento das diretrizes definidas pela Instituição referente ao processo de compras e o respectivo acompanhamento dos prestadores de serviços e fornecedores.

4. PROCEDIMENTOS E CONTROLES ADOTADOS PARA GARANTIR OS OBJETIVOS DE SEGURANÇA CIBERNÉTICA

É de extrema importância a disseminação da cultura de segurança cibernética para garantir a integridade, confiabilidade e disponibilidade das informações. Para garantir o cumprimento dos princípios dispostos acima, o BCG-Brasil utiliza diversos meios como as políticas internas, instruções normativas, comunicados corporativos e a realização de treinamentos periódicos de segurança da informação e compliance.

5. CONTROLES ADOTADOS PARA A SEGURANÇA DAS INFORMAÇÕES SENSÍVEIS

O BCG-Brasil possui diversos controles e procedimentos para garantir a segurança das informações sensíveis, conforme descrito nos tópicos abaixo:

5.1 Controle de Acesso e Gerenciamento

A prática de Controle de Acesso e Gerenciamento tem o objetivo de prevenir o acesso de indivíduos não autorizados ao ambiente e aos sistemas, garantindo assim a confidencialidade das informações. O BCG-Brasil segue as boas práticas no sentido de orientar que todos os usuários devem possuir acesso à informação de acordo com as necessidades de negócio. Como controle adicional há a matriz de segregação de função baseada em cargo/função.

O Banco possui procedimentos formalizados e a descrição dos fluxos operacionais para a Concessão, Alteração, Revogação e Gerenciamento de acessos, sendo que para os procedimentos citados acima, é respeitado o princípio de menor privilégio e perfil mínimo restrito de acesso, conforme a matriz de segregação de função. Adicionalmente, os procedimentos de Concessão e Alteração devem ser aprovados pelo gestor responsável, *System Owner*, Diretoria Executiva, Compliance e Segurança da informação.

O Banco realiza periodicamente a revisão de acessos, conforme política, que tem como objetivo a atualização dos acessos e permissões, procedimento este, que é coordenado pela Área de Segurança da Informação, sendo o resultado da revisão enviado para a anuência da Diretoria.

5.2 Gerenciamento de Riscos e Tecnologia da Informação

O Banco verifica periodicamente o controle de acessos à internet e controla os aplicativos instalados nos computadores. A área de Tecnologia da informação do Banco Caixa Geral Brasil é a responsável por controlar o acesso à internet. Para isso utiliza ferramenta de filtro de conteúdo para intermediar as requisições de usuários e conteúdo disponível na internet.
Atualizações e instalações de dispositivos, periféricos e softwares são de responsabilidade da área de Tecnologia do Banco Caixa Geral. Usuários comuns não possuem direitos para executar atualizações e ou instalações.

5.3 Segurança de Rede

A segurança de rede é realizada através do monitoramento e gerenciamento da infraestrutura, sendo que o acesso às redes internas e acessos à internet são controlados pela área de Tecnologia da Informação.

5.4 Segurança e gerenciamento de Ativos de Sistemas

Quando disponível, o acesso aos sistemas de informação do BCG-Brasil é integrado com o AD (*Active Directory*), que possui as suas especificidades definidas em procedimento interno.
Para os Sistemas de Informação que não estão integrados com AD, existe um pré-requisito mínimo para as parametrizações de senhas definido em procedimento interno.
Referente ao gerenciamento das parametrizações de segurança, somente a área de Segurança da Informação tem acesso para alterar as configurações de acesso e segurança nos Sistemas de Informação.

5.5 Gestão de Ameaças e Vulnerabilidades de TI

O ambiente possui instalado software de antivírus para a proteção contra vírus, arquivos e softwares maliciosos, atualizados periodicamente.
As atualizações de segurança do Windows são gerenciadas e atualizadas periodicamente.

5.6 Dispositivos e Controles de Mídia

Somente pessoas previamente autorizadas pela Diretoria Executiva tem acesso aos dispositivos móveis e acessos ao leitor de DVD e USB do computador.

5.7 Segurança Física

Os recursos e instalações de processamento de informações críticas para as atividades do BCG-Brasil são mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e recursos para controle de acesso. Os equipamentos críticos possuem proteção contra desastre físico e recursos para combate a incêndio.

O Banco possui sistema para controle do acesso dos colaboradores, prestadores de serviços ou fornecedores aos locais restritos, que são monitorados por câmeras.

6. REGISTRO, ANÁLISE DA CAUSA DOS EFEITOS DE INCIDENTES RELEVANTES E VULNERABILIDADES

O registro, análise dos efeitos de incidentes relevantes são atividades cruciais para minimizar impactos negativos para o BCG-Brasil, a nível operacional e reputacional.

Os eventos de TI são registrados no sistema *SAS e GRC*.

O BCG-Brasil se preocupa com as empresas que prestam serviços para o Banco. As informações recebidas por estas empresas são objeto de NDA (*Non Disclosure Agreement*), contempladas em registro específico e objeto de análise complementar no que se refere a impactos dos efeitos de incidentes e vulnerabilidades.

O Banco entende que é de extrema importância a existência de um procedimento que possibilita a detecção tempestiva e a pronta comunicação de incidentes e vulnerabilidades, assegurando assim, a eficácia das medidas a serem tomadas na sequência. O Banco possui os controles que permitem detectar e identificar os incidentes e vulnerabilidades que afetam o ambiente de Segurança Cibernética.

As responsabilidades em relação ao registro, análise e comunicação dos incidentes estão devidamente detalhadas em normativos específicos.

7. DIRETRIZES GERAIS

7.1 Teste de Continuidade de Negócios

O BCG-Brasil assume o compromisso de manter a continuidade dos negócios em caso de incidentes que possam comprometer o funcionamento normal de suas atividades, através do Programa de Gestão de Continuidade de Negócios (PGCN), sendo constantemente revisado com o objetivo contínuo de melhoria. O programa possui o objetivo de identificar e elaborar os cenários que possam comprometer a continuidade da sua atividade, analisar o seu impacto e promover a resiliência organizacional, dotando a organização da capacidade de prevenir ou, na sua impossibilidade, responder de forma eficaz a estes eventos.

O PGCN é constituído por 04 (quatro) fases – Planejamento, Operação, Avaliação/ Revisão e Melhoria contínua. Estas fases contemplam as responsabilidades dos órgãos responsáveis pela coordenação do programa, as reponsabilidades das áreas envolvidas, os procedimentos para a realização da avaliação/revisão do programa, como testes e relatórios de reporte.

7.2 Prestadores de Serviços de Tecnologia

Os procedimentos e controles voltados à prevenção e ao tratamento de incidentes em relação aos prestadores de serviço de Tecnologia são previamente definidos em contratos. Especificamente em relação aos fornecedores de Infraestrutura e SPB, o Banco recebe mensalmente relatórios com os incidentes ocorridos e, em caso de necessidade, é elaborado um plano de ação, que é acompanhado pela área de Tecnologia até o seu encerramento.

7.3 Classificação da criticidade dos Incidentes

Os incidentes relacionados à Segurança Cibernética podem seguir os fatores de criticidade definidos no Manual de Gestão de Crises, considerando 03 tipos de situação: crítica, de emergência e evento inesperado.

7.3.1 Plano de Ação de Resposta a Incidentes

Caso ocorra um incidente, ele deve ser analisado e, após análise, é elaborado um plano de ação para corrigir e/ou melhorar o ambiente e/ou processo com o objetivo de minimizar a possibilidade de nova ocorrência. A elaboração e acompanhamento do plano de ação são coordenados pela Área de Tecnologia da Informação, com participação de outras Áreas.

8. TREINAMENTO DE SEGURANÇA NO BCG-BRASIL

O BCG-Brasil incentiva e promove uma cultura de segurança dentro da instituição, visando proteger os objetivos citados nesta política, e principalmente proteger a informação.

A cultura de Segurança Cibernética é disseminada internamente através de programas de capacitação ministrados periodicamente para todos os colaboradores, garantindo assim que todos estejam cientes das possíveis ameaças e vulnerabilidades que ocorrerem no âmbito da Segurança Cibernética, bem como quais são os procedimentos que devem ser adotados em casos de incidentes.

O Banco tem consciência que as atividades no âmbito de Segurança Cibernética, estão em constante evolução, sendo assim, os procedimentos e controles relacionados com o tema, devem ser revistos com periodicidade, promovendo uma melhoria contínua do ambiente de Segurança Cibernética do BCG-Brasil.

9. COMPARTILHAMENTO DE INFORMAÇÕES

O BCG-Brasil buscando sempre atuar com transparência e objetivando a melhoria dos seus procedimentos relacionados à Segurança Cibernética, tem o compromisso de compartilhar com o BACEN todos incidentes relevantes, tempestivamente.

10. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO DE NUVEM

Toda contratação de serviços de processamento e armazenamento de dados e de computação em nuvem devem estar aderentes com as diretrizes indicadas na Resolução de Segurança Cibernética do BACEN.

11. MÉTRICAS/INDICADORES DE ACOMPANHAMENTO DO PROCESSO DE SEGURANÇA CIBERNÉTICA

Mensalmente, a área de Tecnologia da Informação disponibiliza o KRI (*Key Risk Indicator*) de acompanhamento de incidentes às áreas de Risco Operacional e Controles Internos do Banco.

12. RELATÓRIO ANUAL

De acordo com a Resolução 4.658 do BACEN, anualmente, até o 31 de março, o Banco deverá emitir um relatório sobre a implementação do plano de ação de respostas a incidentes, com data base de 31 de dezembro do ano anterior ao relatório, contendo:

- A efetividade da implementação das ações a serem desenvolvidas pela instituição para adequar suas estruturas aos princípios e às diretrizes da política de Segurança Cibernética;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- Os incidentes relevantes ocorridos no período;
- Resultado dos testes de continuidade de negócios.

13. DOCUMENTAÇÃO MÍNIMA A SER ARQUIVADA DECORRENTE DA RESOLUÇÃO 4.658

Devem ficar à disposição do Banco Central do Brasil pelo prazo de 05 (cinco) anos:

- A presente Política;
- Ata do Conselho de Administração com a aprovação da Política;
- Documento relativo ao plano de ação e de resposta a incidentes;
- Relatório anual;
- Documentação sobre os procedimentos;
- Documentação que trata no caso de serviços prestados no exterior;
- Os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem;

- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle que visam assegurar a implementação e a efetividade da política se Segurança Cibernética.

14. AVALIAÇÃO

O processo e a Política de Segurança Cibernética estão sujeitos à avaliação de Controles Internos e Auditorias.

15. RESPONSÁVEL PERANTE O BANCO CENTRAL DO BRASIL

O Diretor de Riscos é o responsável pela Política de Segurança Cibernética e, encontra-se cadastrado no sistema do BACEN.

16. NORMATIVOS RELACIONADOS

- Política de Segurança da Informação

- Política Corporativa e Instrução de Serviços de Plano de Continuidade dos Negócios

- BIA – *Business Impact Analysis*

- Manual de Gestão de Crises

- Repostas a incidentes

I. ANEXO

I.I CONCEITOS

Ativo de informação – elemento com valor para o BCG-Brasil, para as suas atividades e para a continuidade destas, incluindo as tecnologias de informação e comunicação (TIC) e os recursos de informação do BGC-Brasil que a apoiam no desempenho das suas funções.

Ameaça – causa potencial de incidente indesejável que pode resultar em danos para o BCG-Brasil, para a sua informação ou sistemas de informação. Estas ameaças podem ser acidentais ou deliberadas.

Colaboradores – qualquer pessoa que seja membro do Conselho de Administração, Diretor Executivo, funcionário, estagiário, prestador de serviços ou mandatário, a título permanente ou ocasional, do BCG-Brasil.

Incidente de segurança de informação – qualquer evento que afete ou possa afetar a integridade, disponibilidade, privacidade, confidencialidade, autenticidade, auditabilidade e/ou fiabilidade da informação ou sistemas de informação do BCG-Brasil, incluindo qualquer ação ou omissão, deliberada ou não, que viole a regulação vigente em matéria de segurança de informação.

Informação – todos os dados e registros, tangíveis ou intangíveis, incluindo voz e imagem, independentemente do seu formato, modo de tratamento, meio de transmissão e tipo de suporte, físico ou lógico, relativos ao BCG-Brasil ou às relações deste com os seus clientes e partes interessadas restantes.

Informação do BCG-Brasil – englobam-se neste conceito:

- toda a informação que é propriedade do BCG-Brasil e aquela que, não sendo da sua propriedade, esteja, para efeitos legais, contratuais ou funcionais, sob a responsabilidade direta ou indireta de qualquer das suas estruturas/áreas;
- todos os processos, sistemas, aplicações, serviços, dispositivos, tecnologias, infraestrutura e demais meios de suporte utilizados para criar, registrar, recolher, processar, usar, armazenar, publicar, comunicar, transmitir, transferir, transportar, proteger, recuperar ou eliminar informação, independentemente da sua localização, física e lógica, e da entidade responsável por tais atividades.

Prestador de Serviços – pessoa física ou jurídica que presta qualquer tipo de serviços ao BCG-Brasil.

Segurança da Informação - preservação adequada da confidencialidade, integridade e disponibilidade da informação; envolve também a capacidade das TIC para resistir, com um adequado nível de confiança, a ações que comprometam a confidencialidade, integridade ou disponibilidade dos dados armazenados, transmitidos ou tratados ou a segurança de serviços conexos da Instituição.

Sistema de Informação – conceito abrangente associado ao uso de tecnologias de informação e comunicação no âmbito dos mais variados processos e procedimentos associados à informação.

Tecnologias de Informação e Comunicação (TIC) – expressão que engloba todas as tecnologias, hardware e software, utilizados para criar, registrar, recolher, processar, usar, armazenar, publicar, comunicar, transmitir, transferir, transportar, proteger, recuperar ou eliminar informação.

Vulnerabilidade de segurança de informação – vulnerabilidade técnica, insuficiência a nível dos controles ou outra condição associada a um ativo ou conjunto de ativos de informação que pode ser explorada ou iniciada por ameaças, podendo dar origem ou potenciar a ocorrência de algum incidente de segurança de informação.

Vulnerabilidade técnica – falha, erro, lacuna, fragilidade, insuficiência ou configuração inadequada de um componente tecnológico que processa, transmite e/ou armazena informação (e.g. sistemas operativos, bases de dados, aplicações, equipamentos de rede) que pode resultar numa quebra de segurança ou de qualquer outra forma potenciar a ocorrência de incidentes de segurança.