DESENVOLVE SP
O BANCO DO EMPREENDEDOR

SÃO PAULO
GOVERNO DO ESTADO

Secretaria da
Fazenda e Planejamento

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Este é um resumo contendo as linhas gerais da Política de Segurança Cibernética – Brasil, em cumprimento à Resolução n° 4.658 (“Resolução 4.658”) do Banco Central do Brasil. Publicado no portal institucional da DESENVOLVE SP

CAPÍTULO I – POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. OBJETIVO

A Política de Segurança Cibernética tem como objetivo atender a Resolução nº 4.658, de 26 de abril de 2018, do Conselho Monetário Nacional (CMN), e estabelecer os princípios, conceitos, valores e práticas que devem ser adotados pela Desenvolve SP para garantir a proteção das informações tratadas pela instituição.

2. CONTEÚDO

Princípios, conceitos, valores e práticas adotados pela Desenvolve SP para garantir a proteção das informações tratadas pela instituição.

3. FINALIDADES

- Proteger a imagem da instituição e a de seus clientes;
- Proteger os sistemas e os dados da instituição e de seus clientes contra acessos indevidos e modificações não autorizadas, assegurando, ainda, que as informações estarão disponíveis a todas as partes autorizadas, sempre que demandadas;
- Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos e a correta resposta a incidentes;
- Garantir a disponibilidade dos recursos que suportam os negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por ataques cibernéticos e vulnerabilidades na segurança;
- Atender os requisitos legais, regulamentares e as obrigações contratuais pertinentes à atividade da instituição;

- Conscientizar, educar e treinar os colaboradores, a partir dos conceitos desta Política de Segurança Cibernética, incluindo também outras normas e procedimentos internos aplicáveis à Segurança Cibernética em suas atividades diárias;
- Estabelecer um Plano de Ação e Resposta a Incidentes (Pari) relacionado à Segurança Cibernética.

4. CONCEITOS

A Segurança Cibernética constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo seu compartilhamento de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

4.1 Conceitos adotados neste documento

- Política de Segurança Cibernética (PSC);
- Política de Segurança da Informação (PSI): documento que complementa esta PSC;
- Plano de Continuidade de Negócios (PCN);
- **Confidencialidade**: garantia de que a informação é acessível somente às pessoas autorizadas;
- **Integridade**: salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- **Riscos Cibernéticos**: riscos de ataques cibernéticos, oriundos de *malware*, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets) e fraudes externas, desprotegendo dados, redes e sistemas da instituição, causando danos financeiros e de reputação consideráveis.

4.1.1 Malwares

- **Vírus**: *software* que causa danos à máquina, rede, *softwares* e banco de dados;
- **Cavalo de Troia**: aparece dentro de outro *software* e cria uma porta para a invasão do computador;
- ***Spyware***: *software* malicioso para coletar e monitorar o uso de informações;
- ***Ransomware***: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

4.1.2 Engenharia social

- ***Pharming***: direciona o usuário para um *site* fraudulento, sem o seu conhecimento;
- ***Phishing***: *links* transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial, para obter informações confidenciais;
- ***Vishing***: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
- ***Smishing***: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
- **Acesso pessoal**: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

4.1.3 Fraudes externas e invasões

Realização de operações por fraudadores, utilizando-se de ataques às plataformas de negócios, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

4.1.4 Ataques DDoS e Botnets

Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da empresa. No caso dos Botnets, o ataque vem de um grande número de computadores

infectados utilizados para criar e enviar *spam* ou vírus, ou inundar uma rede com mensagens, resultando na negação de serviços.

4.1.5 Outros conceitos

- ***Backup* de dados:** atividade que gera uma cópia dos dados armazenados em diferentes localidades;
- **Criptografia:** ciência que define princípios e técnicas para transformação da informação, da sua forma original, para outra ilegível, de forma que a mensagem possa ser conhecida apenas por seu destinatário, tornando-a difícil de ser lida por alguém não autorizado;
- **Computação / armazenamento "em nuvem":** termo utilizado para descrever uma rede de servidores. A nuvem não é uma entidade física, mas uma vasta rede de servidores remotos que são conectados e operam como um único ecossistema. Estes servidores podem ser responsáveis por armazenar e gerenciar dados, executar aplicativos ou fornecer conteúdo ou serviços, como transmissão de vídeos, *webmail*, *software* de produtividade ou mídias sociais. Em vez de acessar arquivos e dados do local ou de um computador pessoal, o usuário pode acessá-los *online*, pela internet.

5. APLICABILIDADE

A Política de Segurança Cibernética é aplicável a todas as unidades e colaboradores (funcionários, estagiários e terceiros) da Desenvolve SP, bem como aos fornecedores de serviços de computação em nuvem.

Terceiros em uso das informações e de ativos da Desenvolve SP também devem estar em conformidade para com as diretrizes desta Política. Como "terceiros" estão incluídos, entre outros:

- Prestadores de serviços de apoio e manutenção;
- Prestadores de serviços de operações relacionadas a sistemas de Tecnologia da Informação (TI), serviços de coleta de dados, operações de atendimento, entre outros;
- Clientes;

- Consultores;
- Auditores;
- Pessoal temporário, estagiários, menores aprendizes e outros contratados de curta duração.

6. PRINCÍPIOS

A proteção e privacidade de dados da própria instituição e dos clientes refletem os valores da Desenvolve SP e reafirmam o compromisso com a melhoria continua da eficácia do processo de Segurança Cibernética para proteção de sistemas e dados. Quanto à coleta e ao tratamento dos dados, são práticas determinantes:

- São coletadas de forma ética e legal, para propósitos específicos e devidamente informados;
- Somente são acessadas por pessoas autorizadas e capacitadas para o seu uso adequado;
- Podem ser disponibilizadas às empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossas diretrizes de segurança e privacidade de dados;
- As informações constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais, somente são fornecidas aos próprios interessados, mediante a solicitação formal, seguindo os requisitos legais vigentes.

7. DIRETRIZES CORPORATIVAS

A Política de Segurança Cibernética estabelece diretrizes que buscam complementar a Política de Segurança da Informação (PSI) da Desenvolve SP, para assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela instituição e por seus clientes.

A Desenvolve SP atua frequentemente no aperfeiçoamento de suas aplicações e de seus códigos fontes, onde executa análises DAST/SAST, efetuadas pelo fornecedor

do sistema transacional dos negócios e de gestão corporativa.

A Desenvolve SP deve implementar controles para reduzir as vulnerabilidades dos processos da instituição à incidentes e para atender aos demais objetivos de segurança cibernética, incluindo:

- a autenticação;
- a criptografia;
- a prevenção e a detecção de intrusões;
- a prevenção de vazamento de informações (da instituição e de clientes);
- a realização periódica de testes e varreduras para detecção de vulnerabilidades e *softwares* maliciosos.

A Desenvolve SP estruturou, como complemento desta PSC e de sua PSI, o Plano de Ação e Resposta a Incidentes (Pari), contendo controles e procedimentos de monitoramento, reporte e resposta a incidentes, incluindo análise da causa e do impacto, com foco principal nos ambientes de produção dos fornecedores de Data Center (acesso pela nuvem) e fornecedor do sistema transacional dos negócios e de gestão corporativa.

A Desenvolve SP deve implementar em sua PSI classificação dos dados e das informações quanto a relevância e nível de confidencialidade. O grau de relevância deve variar entre baixo, médio e alto, de acordo com a importância da informação.

O cumprimento da Política de Segurança Cibernética é de responsabilidade de todos os colaboradores e dos prestadores de serviços, conforme suas atribuições.

8. ESTRUTURA DE GERENCIAMENTO

A Desenvolve SP conta com uma unidade (SUNET) ou função específica para planejar, estabelecer, executar e monitorar as atividades e controles relacionados com Segurança das Informações e Segurança Cibernética. Esta função se reporta diretamente à Diretoria da instituição.

As atividades e os controles de Segurança Cibernética executados sob a

responsabilidade dessa unidade objetivam assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e mantidos ou modificados de acordo com os objetivos estabelecidos por esta Política de Segurança Cibernética.

Os subitens abaixo descrevem os principais processos de gerenciamento.

8.1 Gestão de acessos às informações

Os acessos às informações devem ser controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente e aprovação pelo gestor da informação, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

8.2 Proteção do ambiente

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, por meio de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e assegurar a administração segura de redes de comunicações, incluindo a gestão de serviços contratados de processamento e armazenamento de dados e informações em nuvem.

8.3 Segurança física e lógica

Os equipamentos e as instalações de processamento de informação críticos ou sensíveis são mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os requisitos de segurança de sistemas de informação são identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos, visando a manutenção de sua confidencialidade, integridade e disponibilidade.

Os colaboradores e terceiros da Desenvolve SP devem ser treinados periodicamente sobre os conceitos de Segurança da Informação, por meio de um

programa efetivo de conscientização, executado sob a responsabilidade da SUNET.

8.4 Continuidade de negócios

O processo de gestão de continuidade de negócios relativo a segurança da informação é implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, por meio da combinação de requisitos como operações, funcionários-chave, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres.

Incluem-se, nesse processo, a continuidade de negócios relativos aos serviços providos aos clientes da Desenvolve SP.

Tais diretrizes são detalhadas no MNP – Plano de Continuidade de Negócios, incluindo as diretrizes para a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios.

8.5 Serviços processamento, armazenamento de dados e computação em nuvem

Em conformidade com a Resolução CMN nº 4.658/2018, para a contratação de serviços de terceiros para processamento, armazenamento de dados e computação

em nuvem, a Desenvolve SP assegura um procedimento efetivo para a aderência às regras previstas na regulamentação em vigor.

9. UTILIZAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Para os fins do disposto nesta Política, os serviços de computação em nuvem abrangem a disponibilidade à Desenvolve SP, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à Desenvolve SP implantar ou executar *softwares*, que podem incluir sistemas operacionais e aplicativos

desenvolvidos pela instituição ou por ela adquiridos;

- Implantação ou execução de aplicativos desenvolvidos pela Desenvolve SP, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou
- Execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

A Desenvolve SP, previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, deve adotar procedimentos que contemplem:

- A adoção de práticas de governança corporativa e de gestão, proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas;
- A verificação da capacidade do potencial prestador de serviço para assegurar o cumprimento da legislação e da regulamentação em vigor.

Na avaliação da relevância do serviço a ser contratado, a Desenvolve SP deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado, levando em conta, inclusive, a classificação das informações, realizada em conjunto com o desenvolvimento desta Política.

10. PROCEDIMENTOS E CONTROLES

A Desenvolve SP adota procedimentos e controles para reduzir as vulnerabilidades a incidentes e atender aos demais objetivos de Segurança Cibernética. Os principais procedimentos estão descritos nos subitens abaixo.

10.1 Procedimentos e controles de autenticação

A Desenvolve SP adota controles de autenticação, tanto na rede como nos aplicativos de negócios (exemplos: *Active Directory* para acesso à rede; senha e usuário adicional para acesso os sistemas corporativos).

As senhas para acesso ao sistema transacional dos negócios e de gestão corporativa devem atender aos critérios de complexidade, que protegem a sua descoberta.

10.2 Procedimentos e controles de criptografia e proteção de código-fonte

A Desenvolve SP usa a criptografia em todas as senhas de suas aplicações.

O sistema transacional dos negócios e de gestão corporativa possui software de versionamento para guarda de código fonte, bem como possui backup tanto do código fonte como também das versões dos instaladores das aplicações. O fornecedor deste sistema investe em treinamento de metodologia em desenvolvimento seguro para seus colaboradores e usa programas para análises SAST e DAST de suas aplicações.

10.3 Procedimentos e controles de prevenção e detecção de intrusão

Os fornecedores de Data Center da Desenvolve SP e o fornecedor do sistema transacional dos negócios e de gestão corporativa devem implementar recursos em seus dispositivos de rede e nos sistemas, de forma que permitam a detecção de intrusos, bem como a resposta a incidentes.

A Desenvolve SP possui ferramentas de prevenção e detecção de intrusões (IPS e IDS).

10.4 Procedimentos e controles de prevenção de vazamento de informações

A Desenvolve SP tem como diretriz prevenir e detectar todo e qualquer vazamento de informações sensíveis em seu ambiente de tecnologia. Para isso, adota processos e utiliza recursos que mitigam eventos de vazamento de dados, tais como a utilização de ferramentas de Data Loss Prevention (DLP).

10.5 Realização periódica de testes e varreduras para detecção de vulnerabilidades

A Desenvolve SP adota processos e utiliza recursos que visam minimizar as

vulnerabilidades em seu ambiente, tais como a utilização da ferramenta especializado em análise de vulnerabilidades, desenvolvido para verificar redes de computadores, aplicativos, switches, computadores, servidores e outros equipamentos. Dentre os diversos tipos de identificadores de vulnerabilidades destacam-se a varredura de portas, a enumeração de rede e o *service scanners*.

10.6 Proteção contra *softwares* maliciosos

A Desenvolve SP utiliza programas específicos para se proteger contra softwares maliciosos, dentre eles o antivírus e as ferramentas VirusScan e AntiSpyware .

Os fornecedores do sistema transacional dos negócios e de gestão corporativa e do Data Center possuem mecanismos de proteção contra vírus maliciosos.

Para toda estrutura de servidores do fornecedor de Data Center, há camada de antivírus.

10.7 Mecanismos de rastreabilidade

A Desenvolve SP possui controles específicos, incluindo os voltados para a rastreabilidade da informação, que buscam garantir a segurança das informações sensíveis. Há controles e procedimentos de geração de logs transacionais de todos os bancos de dados dos ambientes de produção dos sistemas corporativos.

Para o sistema transacional dos negócios e de gestão corporativa, os logs registram os acessos aos sistemas, abertura e fechamento de telas e inclusão/alteração de dados.

10.8 Controles de acesso e segmentação da rede de computadores

Os dados sendo trafegados entre a o fornecedor de Data Center e a Desenvolve SP são protegidos contra acesso indevido.

Para a comunicação entre o fornecedor de Data Center e a Desenvolve SP, a estrutura de link é formada por Link Lan-to-Lan dedicado ao cliente e com dupla abordagem de operadoras, onde em toda estrutura o cliente possui uma VLAN dedicada para segmentação de seu trafego até a chegada do firewall.

Adicionalmente, a estrutura de redes e segurança do Data Center é composta por equipamentos redundantes, onde na camada externa, juntamente com os roteadores de borda, há solução de proteção contra ataques DDoS. A camada de *firewall* é formada por equipamentos que trabalham da Camada 3 à Camada 7 com as devidas regras de liberação ou bloqueio. Juntamente a essa solução, há também os recursos de IPS/IDS e WAF para prevenção de ataques e vazamento de informações por meio de acessos indevidos.

10.9 Procedimentos que garantem a manutenção de cópias de segurança dos dados e das informações

A Desenvolve SP executa backups diários incrementais, bem como semanais e mensais integrais, dos dados produtivos de seus sistemas corporativos. Este *backup* é executado pelo fornecedor de *Data Center*, e fica armazenado em um local distante dos data-centers de produção.

10.10 Procedimentos de monitoramento e controle de incidentes de segurança

O processo de monitoramento e resposta a incidentes está descrito no Capítulo Plano de Ação e Resposta a Incidentes, deste MNP.

11. MONITORAMENTO DE SEGURANÇA, ACESSOS E ATIVIDADES

11.1 Acessos e atividades

- Atividades realizadas no ambiente informatizado da Desenvolve SP, que gerem impacto no negócio da instituição, devem ser registradas (gerar log para consulta quando necessário);
- A geração de logs (trilhas de auditoria) para atividades com impacto no negócio deve abranger os seguintes sistemas e plataformas:
  - Rede (sistema de arquivos);
  - Aplicativos de negócios e portais;
  - Bancos de dados;
  - Demais plataformas avaliadas como relevantes (por possuírem informações sensíveis ao negócio da Desenvolve SP, de acordo com a

classificação das informações).

- No mínimo, as seguintes informações devem ser identificadas e registradas em trilhas de auditoria:
  - Usuário que realizou o acesso;
  - Atividades realizadas no acesso (leitura, escrita, deleção, etc.);
  - Informações que foram alteradas (com histórico da informação anterior à modificação);
  - Plataforma utilizada no acesso.
- O acesso de profissionais de TI ao ambiente de produção dos sistemas e plataformas tecnológicas da Desenvolve SP, quando aplicável, deve gerar trilhas de auditoria. Tais trilhas não podem ser manipuláveis pelos executores das transações.

12. DIVULGAÇÃO

- A Política deve ser divulgada a todos os colaboradores da Desenvolve SP e estar disponível na rede da instituição para consulta a qualquer momento;
- A Desenvolve SP deve divulgar, aos prestadores de serviços e outras pessoas que possam acessar informações de sua propriedade ou custódia, um resumo contendo as linhas gerais desta Política.